PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-067336
(43)Date of publication of application : 07.03.2003

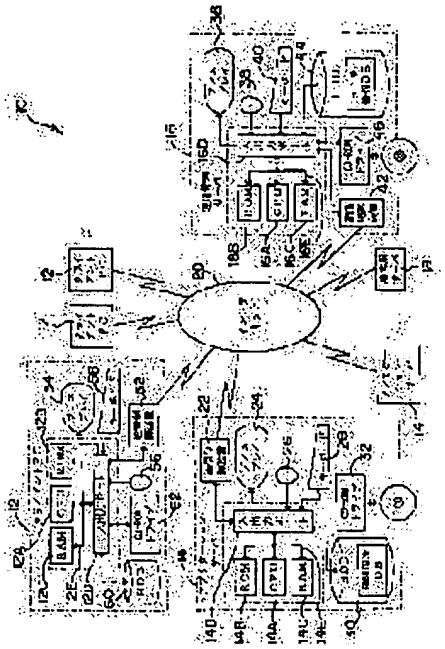
(51)Int.Cl. G06F 15/00

(21)Application number : 2001-255996
(22)Date of filing : 27.08.2001

(71)Applicant : BANK OF TOKYO-MITSUBISHI LTD
(72)Inventor : NAKAMORI YUKIO
KAMEDA HIROKI

(54) COMPUTER SYSTEM AND USER MANAGEMENT METHOD

(57)Abstract:
PROBLEM TO BE SOLVED: To control use of a system by an individual user according to use authority decided to each the individual user without impairing maintainability and security.
SOLUTION: When transmitting a user ID or the like to an operation management server 16 through a PC 12 to request login in use of an MI system 10 including a plurality of application systems realized by individual servers 14, the operation management server 16 issues a ticket after checking the user ID, and displays a menu screen capable of being used by only the application system whose use authority the user has, on a display 54. Various functions provided by the individual application system are used by transmitting the tickets to the corresponding server 14, and the server 14 authenticates the user by the ticket, and provides the requested function only when the user has the use authority of the requested function.



LEGAL STATUS

[Date of request for examination]	27.08.2001
[Date of sending the examiner's decision of rejection]	14.06.2005
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	
[Date of registration]	
[Number of appeal against examiner's decision of rejection]	
[Date of requesting appeal against examiner's decision of rejection]	
[Date of extinction of right]	

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]
[Claim 1] The computer connected with the terminal operated by the user through the communication line It realizes by performing the program group containing two or more sorts of application programs. User Information for being the computer system constituted including two or more sorts of application systems, and checking each available user for said computer system, A 1st storage means to memorize the 1st authority information for specifying said application system with which said each user has two or more use authority among the application systems of a seed, The use authority of each user about two or more sorts of functions who can provide for a user among said application systems which are seeds is established corresponding to each application system which is not fixed. The inside of two or more sorts of functions with which a corresponding application system can provide a user, A 2nd storage means to memorize the 2nd authority information for specifying the function in which each user who has the use authority of said application system has use authority, Based on User Information memorized by said 1st storage means, an user validation is performed to a log in demand of the user to said computer system. A check / authorization means to permit use to the user who has checked that he was a just user only about the application system with which said user has use authority based on said 1st authority information, The application system with which the preparation and said 2nd storage means are established Computer system characterized by providing said user only with the function in which said user has use authority, based on the 2nd authority information memorized by 2nd storage means by which a self-system corresponds to the user who is demanding use of the function with which a user can be provided.
[Claim 2] Said check / authorization means is computer system according to claim 1 characterized by permitting use only about the application system with which it is that the user who has checked that he was said just user displays as alternative only the application system which has use authority on a menu screen for a user to demand use of each application system, and said user has use authority.
[Claim 3] The application system with which said 2nd storage means is established As opposed to the user who is demanding use of the function with which a self-system can provide a user [whether said user displays as alternative only the function to have use authority on a screen for a user to demand use of the function in which said offer is possible, and] Or computer system according to claim 1 characterized by providing said user only with the function in which said user has use authority, by reporting that it is outside use authority when use of the function in which said user does not have use authority is demanded by said user.
[Claim 4] When the level of the use authority of the user about the function with which a corresponding application system can provide a user is classified into two or more classes, said 2nd authority information The information showing to any of two or more of said classes each user who has the use authority of said application system belongs, Or computer system according to claim 1 characterized by being the information which means respectively whether each user who has the

use authority of said application system has use authority about each function with which a corresponding application system can provide a user.
[Claim 5] The application system with which said 2nd storage means is established is computer system according to claim 1 characterized by judging whether said user has the use authority of the function in which use is demanded whenever use of which function of two or more sorts of functions with which a self-system can provide a user is demanded by the user.
[Claim 6] As opposed to the user who has checked that said check / authorization means was a just user The ticket information for using, in case said user uses the application system with which said user has use authority is given. Each of two or more sorts of said application systems Because the user who is demanding use of the function with which a self-system can provide a user judges whether just ticket information is possessed Computer system according to claim 1 characterized by judging whether you are the just user to whom the user who is demanding said use has the use authority of a self-system.
[Claim 7] Said check / authorization means is computer system according to claim 6 characterized by judging whether ticket information with said just user is possessed based on whether when said ticket information with which two or more each of the application system of a seed was transmitted through said terminal from said user is decrypted with a public key, said predetermined information is reproduced using the information which enciphered predetermined information with the private key as said ticket information.
[Claim 8] Computer system according to claim 6 characterized by having further a failure ticket offer means to give a user the ticket information for failures usable when abnormalities arise for said check / authorization means, in case said user uses an application system by adding said user's user ID to a log in demand of the user to said computer system.
[Claim 9] The computer connected with the terminal operated by the user through the communication line It realizes by performing the program group containing two or more sorts of application programs. User Information for being the user management approach applicable to the computer system constituted including two or more sorts of application systems, and checking each available user for said computer system, While memorizing the 1st authority information for specifying said application system with which said each user has two or more use authority among the application systems of a seed for the 1st storage means For said 2nd storage means by which two or more use authority of each user about two or more sorts of functions who can provide for a user among the application systems of a seed was established corresponding to each application system which is not fixed The inside of two or more sorts of functions with which a corresponding application system can provide a user, The 2nd authority information for specifying the function in which each user who has the use authority of said application system has use authority is memorized. Based on User Information memorized by said 1st storage means, an user validation is performed to a log in demand of the user to said computer system. Use is permitted to the user who has checked that he was a just user only about the application system with which said user has use authority based on said 1st authority information. As opposed to the application system with which said 2nd storage means is established The user management approach characterized by providing said user only with the function in which said user has use authority, based on the 2nd authority information memorized by the 2nd storage means when use of the function in which said application system can be offered is demanded by the user.

[Translation done.]

* NOTICES *

JPO and NCIPI are not responsible for any

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention] This invention relates to computer system and the user management approach, and relates to the user management approach applicable to the computer system especially constituted including two or more sorts of application systems, and this computer system.

[0002]
[Description of the Prior Art] Eliminating unjust use of the others other than the valid user registered beforehand in computer system Generally User Information (for example, user ID and a password) of a valid user is memorized beforehand. Transmission of User Information is required of the user who is going to log in to computer system. It is carried out, when User Information transmitted from the user side through the terminal of a personal computer (PC) etc. is collated with User Information memorized beforehand and the user who is going to log in judges whether it is a valid user. The function (service) which computer system offers turns into that only the user who was judged to be a valid user and has logged in normally is available.
[0003] Moreover, in the various functions which computer system offers, the function in which use is permitted only to some users of the valid users may exist. In such a case, computer system memorizes beforehand the authority information which specifies each user's use authority over an offer function, and it is constituted so that only the function in which each user has use authority to each user who logged in may be offered with reference to the authority information of the user who logged in. In addition, as for authority information, it was common to have been saved in a single database (DB) with User Information.
[0004]
[Problem(s) to be Solved by the Invention] By the way, although mechanization of business is considerably tackled for some time in the financial institution for the purpose of the improvement in service to the improvement in effectiveness and the customer of business The application system of the a large number kind which carried out mutually-independent for supporting execution of mutually different business since the business in a financial institution is various exists. In order to use each application system, the dedicated terminal prepared for each application system of every needed to be operated, and it needed to log in to each application system according to the individual. For this reason, unifying various kinds of application systems and building single computer system is examined.
[0005] In however, the case of having unified two or more sorts of application systems which offer service which is mutually different as mentioned above, and having built single computer system etc. For example, although the authority information on a certain application system is the information showing to any of which class each user belongs when it classifies the level of a user's use authority into two or more classes, it receives. Another authority information on an application system it is the information which specifies respectively whether each user has use authority about all the functions with which an application program can provide a user -- etc. -- it is [like] different for each application system of every in many cases, considering the system of authority

information itself.
[0006] In such a case, since the DS of the information saved at DB will become very complicated supposing it unifies the authority information corresponding to each application system and saves with User Information at single DB for example, a new addition of a user or modification (for example, modification of the number of classes into which the level of use authority is classified --) of the DS of the authority information corresponding to a specific application system The activity at the time of performing addition of a table which set each user's use authority to the detail becomes very complicated, and there is a problem that maintenance nature falls sharply.
[0007] Moreover, if unitary management of the information (authority information and User Information corresponding to each application system) for managing use of computer system by making each user into a unit as mentioned above is carried out at DB, since the others other than a valid user will become possible [also carrying out unjust use of the computer system freely] by rewriting the information which invades into computer system and is kept by above DB, it is not desirable from the field of security.
[0008] It is the purpose to acquire the computer system and the user management approach of realizing that this invention controls use of the system by each user according to the use authority which accomplished in consideration of the above-mentioned fact, and was defined for each user of every, without spoiling maintenance nature and security nature.
[0009]
[Means for Solving the Problem] The computer system applied to invention according to claim 1 in order to attain the above-mentioned purpose The computer connected with the terminal operated by the user through the communication line It realizes by performing the program group containing two or more sorts of application programs. User Information for being the computer system constituted including two or more sorts of application systems, and checking each available user for said computer system, A 1st storage means to memorize the 1st authority information for specifying said application system with which said each user has two or more use authority among the application systems of a seed, The use authority of each user about two or more sorts of functions who can provide for a user among said application systems which are seeds is established corresponding to each application system which is not fixed. The inside of two or more sorts of functions with which a corresponding application system can provide a user, A 2nd storage means to memorize the 2nd authority information for specifying the function in which each user who has the use authority of said application system has use authority, Based on User Information memorized by said 1st storage means, an user validation is performed to a log in demand of the user to said computer system. A check / authorization means to permit use to the user who has checked that he was a just user only about the application system with which said user has use authority based on said 1st authority information, The application system with which the preparation and said 2nd storage means are established It is characterized by providing said user only with the function in which said user has use authority, based on the 2nd authority information memorized by 2nd storage means by which a self-system corresponds to the user who is demanding use of the function with which a user can be provided.
[0010] The computer connected with the terminal (you may be the client computer which consists of PC etc., and may be the terminal of a TSS terminal unit etc.) operated by the user through the communication line is realized by performing the program group containing two or more sorts of application programs, and the computer system concerning invention according to claim 1 is constituted including two or more sorts of application systems (system realized because a computer executes each application program). In addition, although you may be a single computer, since the direction of a configuration of sharing and performing said program group by two or more computers can distribute the load which joins a computer, the computer which performs said program group has it. [desirable]
[0011] User Information for checking each available user for computer system in invention according

to claim 1, And the 1st authority information for specifying the application system with which each user has use authority among two or more sorts of application systems is memorized by the 1st storage means. Check / authorization means receives a log in demand of the user to computer system. An user validation is performed based on User Information memorized by the 1st storage means, and use is permitted to the user who has checked that he was a just user only about the application system with which the user has use authority based on the 1st authority information.
[0012] In addition, as User Information, the information on user ID, a password, etc. is applicable, for example. Moreover, other approaches may be used for permitting use only about the application system with which the user has use authority, although it is realizable when the user who has checked that he was a just user displays as alternative only the application system which has use authority on a menu screen for a user to demand use of each application system as indicated to claim 2.
[0013] Since the 1st authority information is the information showing the use authority of each user who makes each application system a unit and it is the information which makes each user a unit also about User Information, each DS of such information memorized by the 1st storage means is easy. Therefore, an available user is newly added for the computer system concerning this invention, or rewriting of the information aiming at newly adding an application system etc. is also easy, and it excels in maintenance nature.
[0014] In invention according to claim 1, moreover, the inside of two or more sorts of application systems, The 2nd storage means is established corresponding to each application system whose use authority of each user about two or more sorts of functions who can provide for a user is not fixed. The 2nd authority information for specifying the function in which each user who has the use authority of said application system among two or more sorts of functions with which a corresponding application system can provide a user has use authority as this 2nd storage means is memorized. And the application system with which the 2nd storage means is established provides said user only with the function in which said user has use authority, based on the 2nd authority information memorized by 2nd storage means by which a self-system corresponds to the user who is demanding use of the function with which a user can be provided. Thereby, according to the use authority (use authority specified using the 1st authority information and the 2nd authority information) defined for each user of every, use of the system by each user is controllable.
[0015] In addition, the application system with which the 2nd storage means is established Providing a user only with the function in which this user has use authority, to the user who is demanding use of the function with which a self-system can provide a user As indicated to claim 3, to said user on for example, a screen for a user to demand use of the function in which said offer is possible Other approaches may be used, although it can realize by reporting that it is outside use authority when use of the function in which display as alternative only the function in which said user has use authority, or said user does not have use authority is demanded by said user.
[0016] Since the use authority of each user about two or more sorts of functions who can provide for a user is the authority information on each application system proper which is not fixed, the 2nd authority information As an informational system will be different according to the class of function which an application system offers etc., for example, being indicated to claim 4 When the level of the use authority of the user about the function with which a corresponding application system can provide a user is classified into two or more classes If it may be the information showing to any of two or more of said classes each user who has the use authority of said application system belongs It may be the information which means respectively whether each user who has the use authority of said application system has use authority about all the functions with which a corresponding application system can provide a user.
[0017] On the other hand, in invention according to claim 1, since the 2nd storage means is established corresponding to each of the application system whose use authority of each user about two or more sorts of functions who can provide for a user is not fixed, as compared with the case

where the 2nd authority information memorized by each 2nd storage means unifies the 2nd authority information on all application systems, DS becomes easy. Therefore, rewriting of the 2nd authority information aiming at changing the information system of the 2nd authority information corresponding to a specific application system etc. is also easy, and it excels in maintenance nature.

[0018] Moreover, the thing for which a specific user uses the specific function which a specific application system offers in invention according to claim 1 The 1st authority information memorized by the 1st storage means serves as contents showing said specific user having the use authority of said specific application system. And the 2nd authority information memorized by the 2nd storage means corresponding to said specific application system becomes possible for the first time because they are the contents showing said specific user having the use authority of said specific function. Thus, since the 1st storage means and the 2nd storage means distribute and the information which specifies each user's use authority is managed, it excels in invention according to claim 1 also at security nature.
[0019] Therefore, according to invention according to claim 1, it can realize controlling use of the system by each user according to the use authority defined for each user of every, without spoiling maintenance nature and security nature.
[0020] The application system with which, as for invention according to claim 5, the 2nd storage means is established in invention according to claim 1 is characterized by judging whether the user has the use authority of the function in which use is demanded, whenever use of which function of two or more sorts of functions with which a self-system can provide a user is demanded by the user.
[0021] In invention according to claim 5, the application system with which the 2nd storage means is established Since it judges whether said user has the use authority of the function in which use is demanded whenever use of which function of two or more sorts of functions which can be offered is demanded by the user A user's use authority over the function in which an application system can be offered It can prevent certainly being unjustly used by the user to whom it becomes possible to manage as a unit each function in which each application system can be offered, and use authority does not have each function in which each application system can be offered.
[0022] Invention according to claim 6 is set to invention according to claim 1. Said check / authorization means The ticket information for using, in case said user uses the application system with which said user has use authority to the user who has checked that he was a just user is given. Each of said application system which are seeds It is characterized by judging whether you are the just user to whom the user who is demanding said use has the use authority of a self-system because the user who is demanding use of the function with which a self-system can provide a user judges whether just ticket information is possessed.
[0023] Ticket information is given to the user who has checked that he was a just user in invention according to claim 6. Each of two or more sorts of application systems Because a user judges whether just ticket information is possessed Since said user judges whether you are a just user, the user who does not possess just ticket information Direct access is carried out to the specific application system which does not have use authority, and this can be prevented also when it is going to use unjustly the function which this specific application system offers. Therefore, it can prevent that unjust use of the computer system is carried out, without passing through the check of being a just user by check / authorization means according to invention according to claim 6.
[0024] In addition, in invention according to claim 6, as indicated to claim 7, the information which enciphered predetermined information with the private key as ticket information can be used for check / authorization means. In this case, when each of two or more sorts of application systems decrypts the ticket information transmitted through the terminal from the user with a public key, it can judge whether the user possesses just ticket information based on whether predetermined information is reproduced.

[0025] In invention according to claim 6, when abnormalities arise for check / authorization means, to the log in demand of the user to computer system, invention according to claim 8 is adding said user's user ID, and in case said user uses an application system, it is characterized by having further a failure ticket offer means to give a user the usable ticket information for failures.
[0026] In this invention, when abnormalities arise for check / authorization means for the reason of a certain abnormalities having occurred to the computer which functions as a check / authorization means and the log in demand to computer system is no longer received normally, there is un-arranging [that each application system itself lapses into the condition that a just user can use no application systems even if it is in an available condition]. On the other hand, in invention according to claim 8, since the ticket information for failures is given to a user by the failure ticket offer means when abnormalities arise for check / authorization means, also when abnormalities arise for check / authorization means, a just user can avoid lapsing into the condition that no application systems can be used.
[0027] The user management approach concerning invention according to claim 9 The computer connected with the terminal operated by the user through the communication line It realizes by performing the program group containing two or more sorts of application programs. User Information for being the user management approach applicable to the computer system constituted including two or more sorts of application systems, and checking each available user for said computer system, While memorizing the 1st authority information for specifying said application system with which said each user has two or more use authority among the application systems of a seed for the 1st storage means For said 2nd storage means by which two or more use authority of each user about two or more sorts of functions who can provide for a user among the application systems of a seed was established corresponding to each application system which is not fixed The inside of two or more sorts of functions with which a corresponding application system can provide a user, The 2nd authority information for specifying the function in which each user who has the use authority of said application system has use authority is memorized. Based on User Information memorized by said 1st storage means, an user validation is performed to a log in demand of the user to said computer system. Use is permitted to the user who has checked that he was a just user only about the application system with which said user has use authority based on said 1st authority information. As opposed to the application system with which said 2nd storage means is established When use of the function in which said application system can be offered is demanded by the user Since it is characterized by providing said user only with the function in which said user has use authority, based on the 2nd authority information memorized by 2nd storage means to correspond It can realize controlling use of the system by each user like invention according to claim 1 according to the use authority defined for each user of every, without spoiling maintenance nature and security nature.
[0028]
[Embodiment of the Invention] Hereafter, an example of the operation gestalt of this invention is explained to a detail with reference to a drawing. In order to support the various business of a financial institution, the computer system 10 (the MI system 10 is called hereafter) installed in the financial institution is shown in drawing 1 .
[0029] Two or more sets of a client PC 12 (equivalent to the terminal of this invention) and application servers 14, the operational administration server 16, and the server 18 for failures of the a large number base installed in each post of a financial institution are mutually connected through intranet 20, and the MI system 10 is constituted. In addition, the application server 14, the operational administration server 16, and the server 18 for failures support the computer according to claim 1 respectively.
[0030] Each application server 14 consists of a workstation or a general-purpose large-sized computer respectively, is equipped with CPU14A, ROM14B, RAM14C, and input/output port 14D, and these are mutually connected through bus 14E, such as an address bus, a data bus, and a

control bus, and it is constituted. CCE (for example, router) 22 connected to intranet 20, a display 24, a mouse 26, a keyboard 28, HDD30, and CD-ROM drive 32 that reads information from CD-ROM are respectively connected to input/output port 14D as various kinds of input/output equipment.
[0031] In the financial institution, although mechanization of business was considerably tackled for some time for the purpose of the improvement in service to the improvement in effectiveness and the customer of business, since the business in a financial institution was various, two or more sorts of application systems which carried out mutually-independent for supporting mutually different business existed. In order that each application server 14 may realize the application system of ****** from the first, it is the computer formed corresponding to each application system, and a mutually different application program for performing processing (application process) which supports specific corresponding business by CPU14A is beforehand installed in HDD30 of each application server 14.
[0032] The MI system 10 concerning this operation gestalt is a system built by unifying two or more sorts of application systems realized by each application server 14, the user of the MI system 10 is logging in to the MI system 10 through the single client PC 12 connected to intranet 20, and using the function of the arbitration which the application system of arbitration offers is also constituted possible.
[0033] However, in the MI system 10, use authority is granted to each user only about the function which each application system needs for each user's business among each function with which a user can be provided. Specifically, a part of management of a log in of each user to the MI system 10 and management (management of the use authority of each user who makes each application system a unit) of the use authority of each user about each function who can offer the MI system 10 are performed by the operational administration server 16. In addition, management of the finer use authority for use of each application system is performed by each application system (each application server 14).
[0034] The operational administration server 16 consists of a workstation or a general-purpose large-sized computer, is equipped with CPU16A, ROM16B, RAM16C, and input/output port 16D, and these are mutually connected through bus 16E, such as an address bus, a data bus, and a control bus, and it is constituted. A display 36, a mouse 38, a keyboard 40, the communication controller (for example, router) 42 connected to intranet 20, HDD44, and CD-ROM drive 46 which reads information from CD-ROM are respectively connected to input/output port 16D as various kinds of input/output equipment. MI operational administration program for performing MI operational administration processing (it mentioning later for details) by CPU16A of the operational administration server 16 in the operational administration server 16 is installed in HDD44.
[0035] The server 18 for failures is a computer which consists of a workstation or a general-purpose large-sized computer like the operational administration server 16, and when a failure occurs in the operational administration server 16 and a log in to the MI system 10 becomes difficult, it performs processing for a user to log in to the MI system 10 instead of the operational administration server 16.
[0036] Moreover, a client PC 12 consists of a personal computer (PC), is equipped with CPU12A, ROM12B, RAM12C, and input/output port 12D, and these are mutually connected through bus 12E, such as an address bus, a data bus, and a control bus, and it is constituted. CCE (for example, router) 52 connected to intranet 20, a display 54, a mouse 56, a keyboard 58, HDD60, and CD-ROM drive 62 that reads information from CD-ROM are respectively connected to input/output port 12D as various kinds of input/output equipment. MI system use program for performing MI system use processing (it mentioning later for details) by CPU12A of a client PC 12 in a client PC 12 is installed in HDD60.
[0037] Next, as an operation of this operation gestalt, registration of authority information is explained first. The User Information database (DB) for managing use authority of each user who makes a unit management and each application system of a log in of each user to the MI system 10

is memorized by HDD44 of the operational administration server 16. Information as shown in the next table 1 is memorized about each user by this User Information DB.

[0038]

[Table 1]

< ユーザ情報ＤＢの内容(一例) >

項目	内容
ユーザＩＤ	xxxxxxxx
パスワード	yyyyyyyy
所属部署ＩＤ	zzzz
役職ＩＤ	wwww
その他の属性情報	vvvv
利用権限を有するアプリケーション	アプリＡ
	アプリＢ
	:

[0039] In Table 1, "user ID" is the information for identifying each user who has the use authority of the MI system 10, and the information, the "their affiliation post ID", "Executive ID", and "the attribute information on other" that a "password" is used for user authentication on the occasion of a log in are their affiliation post of each user, an executive, and the information for in addition to this (for example, management partition of business which each user performs) identifying. Moreover, in the MI system 10 concerning this operation gestalt, use authority is granted only about the application system required for execution of each user's business to each user. For this reason, a registration setup of ID of the application system with which each user has use authority is carried out at "the application which has use authority." Registration of the information of each user to User Information DB is performed at its post which has managed the MI system 10 whole.

[0040] In addition, HDD44 with which the other information to the 1st authority information on this invention is respectively equivalent to User Information of this invention, and remembers User Information DB to be supports ["the application which has use authority"] the 1st storage means of this invention among various kinds of information mentioned above. Since only the use authority of each user who makes an application system a unit is memorized by User Information DB so that clearly also from Table 1, the information memorized by User Information DB is very easy DS, and when a use user is added or a new application system is added, the maintenance of updating information can be performed easily.

[0041] Moreover, in order to face using for HDD30 of each application server 14 the application system with which each user corresponds and to manage finer use authority, the authority information DB into which the information for specifying each user's use authority was registered is memorized. In addition, the authority information DB is equivalent to the 2nd authority information on this invention, and HDD30 of each application server 14 which memorizes the authority information DB supports the 2nd storage means of this invention. The contents (system of the information which specifies use authority) of this authority information DB are different with each application system (each application server 14).

[0042] That is, with this operation gestalt, the application system (henceforth a RTGS system) for supporting the business about the checking account of the Bank of Japan or settlement of a national bond is contained in each application system realized by each application server 14. In this RTGS system, as shown in the next table 2 as an example, the use authority granted to a user is beforehand patternized for every its affiliation post of a user and executive using the two-dimensional matrix, and the pattern of the use authority defined for every its affiliation post and executive is memorized as authority pattern information by the authority information DB on a RTGS system.

[0043]
[Table 2]
〈 ＲＴＧＳシステムにおける利用権限のパターン 〉

	部署A		部署B		…
	役職A	役職B	役職A	役職B	…
機能a		○		○	…
機能b	○	○		●	…
機能c	●	○	○	○	…
:	:	:	:	:	:

[0044] However, since, as for "-", good is given and, as for "O", the same use authority is granted to a user with its affiliation post and an executive same possible [reference and updating] therefore in a RTGS system only for reference A setup of the use authority to each user using a RTGS system clear [from the User Information setting screen shown as an example] to drawing 2 -- as -- one's affiliation post (drawing 2 -- a "clubroom name" and a "group") -- It completes in inputting information, such as an executive (drawing 2 "authority") and user ID (login ID). To the authority information DB on a RTGS system The information (for example, its affiliation post ID, Executive ID, etc.) for specifying whether each user's use authority supports which pattern corresponds with user ID, and is memorized.
[0045] Moreover, in each application system of the MI system 10, the application system (henceforth a RAPID system) for supporting the business about a circle fund is contained. In this RAPID system, creation of the pattern of use authority is enabled regardless of its affiliation post of a user and an executive at arbitration.
[0046] That is, the functional name display column 70 is formed in screen right-hand side, and the authority pattern setting screen of the RAPID system shown in drawing 3 as an example is choosing a specific function as this functional name display column 70 out of the function by which it was indicated by the list, and is added to the pattern of the use authority which the use authority of the selected function is creating. The pattern number set as the pattern number input column 72 prepared in the left-hand side of an authority pattern setting screen is added as ID, and the pattern of the created use authority is memorized as authority pattern information by the authority information DB on a RAPID system.
[0047] And a setup of the use authority to each user using a RAPID system So that clearly also from the User Information setting screen shown in drawing 4 as an example User ID and one's affiliation post, In addition to information, such as an executive, the pattern of the use authority set as this user is completed by setting it as the setting column 74 by the pattern number (ID). To the authority information DB on a RAPID system The information on the pattern ID for specifying whether each user's use authority supports which pattern etc. corresponds with user ID, and is memorized. In addition, since the pattern of use authority can be created regardless of its affiliation post of a user and an executive in a RAPID system, it is also possible to create a pattern for each user of every if needed, and each user's use authority can be set up more finely.
[0048] Moreover, in each application system, the application system (henceforth a PYRAMID system) for supporting the business about derivatives is contained. In this PYRAMID system, two or more categories as shown in the next table 3 exist as use authority granted to a user, and the convention approach of use authority is different for every category.
[0049]
[Table 3]

権限の種類	権限の内容
オペレーション権限	各種オペレーション画面を操作する権限
取引オペレーション権限	約定データに対するオペレーション権限
マーケットデータオペレーション権限	マーケットデータを登録/更新する権限
:	:

[0050] For example, among each category shown in Table 3, about "operation authority", the use authority of the various functions belonging to "operation authority" is patternized respectively, and the pattern of the use authority of the various functions for each operation authority class of every is memorized [classes / corresponding to each executive of an assistant / dealer / chief / three / operation authority] as operation authority pattern information by the authority information DB on a PYRAMID system.
[0051] A setup of the use authority about the "operation authority" to each user using a PYRAMID system It is carried out by specifying whether each user belongs to which class of the three operation authority classes. When the specified operation authority class corresponds with user ID and is memorized by the authority information DB on a PYRAMID system The use authority (authority to operate various operation screens (only reference referring to /and updating)) of the various functions belonging to each user's "operation authority" is registered.
[0052] moreover, about "dealings operation authority" While the use authority of the various functions belonging to "dealings operation authority" is respectively patternized about three dealings operation authority classes corresponding to each executive of an assistant / dealer / chief The use authority (for example, currency authority, goods authority [handling / authority etc.]) relevant to "dealings operation authority" [handling / authority etc.] The management partition of business which their affiliation post and each user perform is defined as a unit. The use authority to make each pattern, one's affiliation post, and management partition of use authority for every dealings operation authority class into a unit is memorized as dealings operation authority information by the authority information DB on a PYRAMID system.
[0053] For this reason, it is related with "dealings operation authority." While each user using a PYRAMID system specifies whether it belongs to which class of the three dealings operation authority classes When it is carried out by specifying one's affiliation post and a management partition, the dealings operation authority class, their affiliation post, and management partition which were specified correspond with user ID and the authority information DB on a PYRAMID system memorizes Various kinds of use authority (various kinds of operation authority over agreement data) to belong to each user's "dealings operation authority" is registered.
[0054] thus, about the fine use authority of each user who makes a unit the various functions in which each application system can be offered Since HDD30 of each corresponding application server 14 memorizes and it dissociates for every application system While the DS of the information (information memorized to the authority information DB on each application server 14) which specifies use authority becomes easy as compared with the case where unitary management of the use authority of each user about the MI system 10 is carried out The system of the information which specifies use authority can be defined freely, without being influenced of other application systems. Therefore, a change of the system of the information which specifies maintenance and use authority, such as an addition of a use user, itself etc. can be made comparatively easily.
[0055] Then, with reference to the flow chart of drawing 5 - drawing 7 , in case a user uses the MI system 10, the processing performed by each computer is explained. If a user directs use of the MI system 10 to a client PC 12, when MI system use program is performed by CPU12A of a client PC 12, MI system use processing shown in drawing 5 will be performed by the client PC 12.
[0056] By this MI system use processing, the user ID for logging in to the MI system 10 and the input of a password are first requested from a user by displaying MI log in screen as shown in

drawing 8 as an example in step 100 on the display 54 of a client PC 12. At the following step 102, it judges whether activation of a log in was directed by the user, and it stands by until a judgment is affirmed.

[0057] The carbon button 80 for directing the input column 78 for entering the input column 76 for inputting user ID and a password and activation of a log in is formed in MI log in screen. If user ID is entered into the input column 76, a password is respectively entered into the input column 78 and a carbon button 80 is further clicked because a user operates the keyboard 58 and mouse 56 of a client PC 12, a log in to the MI system 10 will be required by the judgment of step 102 being affirmed, shifting to step 104, and transmitting the user ID and the password which were entered to the operational administration server 16 through intranet 20. At step 106, it judges whether the response to a log in demand was received from the operational administration server 16, and it stands by until a judgment is affirmed.

[0058] On the other hand, at the operational administration server 16, MI operational administration processing shown in drawing 6 is always performed by MI operational administration program being performed by CPU16A. In this MI operational administration processing, it judges whether a certain demand was received from other computers of client PC12 grade at step 170, and it stands by until a judgment is affirmed. If the judgment of step 170 is affirmed, it will shift to step 172, and the contents of the demand which received from other computers are judged, and it branches according to a judgment result.

[0059] When the demand which received is a log in demand from the above clients PC 12, it shifts to step 174 from step 172. In addition, step 174 - step 190 support check / authorization means of this invention.

[0060] That is, the user ID and the password which were received from the client PC 12 are used as a key, and User Information DB is searched with step 174. Moreover, at the following step 176, it judges whether the combination of the user ID which received, and a password is registered into User Information DB based on the result of retrieval of step 174. When this judgment is denied, since it can judge that this log in demand is not a demand from the valid user of the MI system 10, it shifts to step 190, and after transmitting the error response which notifies the purport which cannot receive a log in by the reasons of user ID un-registering, a password error, etc. to the client PC 12 of log in demand origin, it returns to step 170.

[0061] Moreover, when the judgment of step 176 is affirmed, after reading the information (one's affiliation post ID, executive ID, etc.) which is matched with user ID and a password and is memorized by User Information DB from User Information DB and storing temporarily at RAM16C etc., it shifts to step 178, and user ID which received is used as a key, and a log in managed table is searched. Moreover, at step 180, it judges whether the user ID which received is registered into the log in managed table based on the result of retrieval of step 178.

[0062] Since this log in managed table can be judged to be the table which registers into the MI system 10 the user ID of all the users that are doing the current log in, and to be a duplex log in when the judgment of step 180 is affirmed, after it transmits the error response which notifies a duplex log in to the client PC 12 of log in demand origin, it returns to step 170 in step 190. Moreover, when the judgment of step 180 is denied, the log in demanded is judged to be the just log in demand from a valid user, matches the user ID which received previously with information, such as log in time, in step 182, and carries out additional registration at a log in managed table.

[0063] At the following step 184, the ticket which is needed in case the user who logs in uses an application system with use authority based on the information and user ID which read from User Information DB and are stored temporarily is generated. After specifically adding the time of the ticket date of issue, the predetermined Magic WORD (for example, version information) which a user cannot know to the information about users, such as user ID, it is generable by enciphering a series of information with a private key.

[0064] Moreover, at step 186, the menu definition information which specifies MI menu screen (an

example is shown in drawing 9) displayed on the display 54 of the client PC 12 of log in demand origin is generated based on the authority information ("application which has use authority") which reads from User Information DB and is stored temporarily.
[0065] MI menu screen displayed when the user to whom drawing 9 has use authority only about the RTGS system and the RAPID system among each application system of the MI system 10 logs in is shown. Although the carbon buttons 82A-82G which the name of each application system contained in the MI system 10 described are formed in MI menu screen concerning this operation gestalt so that clearly also from drawing 9 Only about the carbon button 82 (the example of drawing 9 carbon buttons 82C and 82D) of the application system with which the user has use authority It is indicated by active so that a user may be selectable as a candidate for use, and the carbon button 82 corresponding to the application system with which the user does not have use authority can be chosen no longer as a candidate for use by being indicated by inactive.
[0066] At step 186, menu definition information is generated so that the above MI menu screens may be displayed on the display 54 of a client PC 12 based on menu definition information. In addition, it replaces with indicating by inactive as mentioned above, and you may make it not display the carbon button 82 corresponding to the application system with which the user does not have use authority.
[0067] And at the following step 188, by transmitting the ticket and menu definition information which were generated to the client PC 12 of log in demand origin, a normal response is returned to a log in demand, and it returns to step 170.
[0068] In MI system use processing (drawing 5), if a certain response is received from the operational administration server 16 within predetermined time or the response from the operational administration server 16 becomes a time-out after requiring a log in at step 104, in step 108, it will judge whether the normal response was received from the operational administration server 16.
[0069] When an error response is received from the operational administration server 16, or when the response from the operational administration server 16 becomes a time-out, a judgment is denied, it shifts to step 112, and a user is notified of the usual log in to the MI system 10 having gone wrong by displaying an error screen on a display 54. And when the error response from the operational administration server 16 is received, based on the received error response, the message which notifies the purport which cannot receive a log in by the reasons of user ID un-registering, a password error, etc. is displayed, or the message which notifies that it is a duplex log in is displayed.

[0070] At the following step 114, it judges whether the failure has occurred in the operational administration server 16 based on whether the response from the operational administration server 16 became a time-out. It stands by until return, user ID, and a password are entered into step 102 and activation of a log in is directed again, when a judgment is denied. In addition, about processing when the judgment of step 114 is affirmed, it mentions later.
[0071] Moreover, when a normal response is received from the operational administration server 16, the judgment of step 108 is affirmed, it shifts to step 110, and the ticket and menu definition information which were received from the operational administration server 16 are memorized to HDD60. Based on the menu definition screen memorized to HDD60, MI menu screen (refer to drawing 9) mentioned above is expressed on a display 54 as the following step 122.
[0072] As mentioned above, since the application system with which, as for MI menu screen, the user does not have use authority can be chosen no longer as a candidate for use, it can prevent that a user uses the application system which does not have use authority. Moreover, also when the user who has the use authority of two or more application systems uses for sequential or juxtaposition two or more application systems which have use authority, it becomes possible to use two or more application systems from the client PC 12 single only by performing once log in actuation of entering user ID and a password and directing a log in, and a single sign-on can be realized.

[0073] At step 124, it judges whether which carbon button in MI menu screen was chosen, and it stands by until a judgment is affirmed. It judges whether when the operator operated the mouse 56 grade and chose which carbon button in MI menu screen, the judgment of step 124 was affirmed, it shifted to step 126, the carbon button chosen by the user was based on whether it is the specific carbon button 82 by which it is indicated by active among carbon buttons 82A-82G, and use of the specific application system which has use authority was chosen by the user.
[0074] When the judgment of step 126 is affirmed, it shifts to step 128. Read the ticket memorized to HDD60 and the information showing the contents of actuation by the user etc. is added to the read ticket. By transmitting to the specific application server 14 corresponding to the carbon button 82 chosen by the user The inside of the various functions which a specific corresponding application system offers, Use of the specific function (for example, function to which the main menu of a specific application system is displayed on a display 54 when the carbon button 82 with which it corresponds on MI menu screen is chosen by the user) corresponding to directions of a user is required. At the following step 130, it judges whether a certain response was received from the application server 14 of a ticket transmission place, and it stands by until a judgment is affirmed.
[0075] On the other hand, at each application server 14, MI application process shown in drawing 7 is respectively performed by the application program installed in HDD30 being performed by CPU14A. In MI application process, it judges whether the information which requires use of a specific function from a client PC 12 at step 210 was received, and it stands by until a judgment is affirmed.
[0076] That a user uses the specific function which a RTGS system offers in this operation gestalt chooses carbon button 82C corresponding to the RTGS system on MI menu screen, and it is in the condition that the menu bar of a RTGS system as shown in drawing 10 as an example is shown on the display 54 by the application server 14 corresponding to a RTGS system, and accomplishes it by displaying a pull down menu and choosing a desired item.
[0077] Moreover, using the specific function which a RAPID system offers, for example chooses carbon button 82D corresponding to the RAPID system on MI menu screen, and it is in the condition that the main menu screen of a RAPID system as shown in drawing 11 as an example is shown on the display 54 by the application server 14 corresponding to a RAPID system, and accomplishes it by making sequential selection of the desired item.
[0078] Using the specific function of a specific application system including displaying on a display 54 the menu shown in drawing 10 or drawing 11 here Whenever a user performs in detail actuation of requiring use of a specific function, the information which requires use of a specific function is transmitted to the application server 14 which corresponds from a client PC 12 according to actuation of a user (step 128 mentioned above). The application server 14 which received information is realized by performing step 212 or subsequent ones by the judgment of step 210 of drawing 7 being affirmed.
[0079] The flow chart (step 212) of drawing 7 It is a flow chart explaining the part into which it is [of the processings performed by each application server 14 whenever it receives the information which requires use of a specific function from a client PC 12] common. Although step 212 or subsequent ones is explained below, without specifying the function in which the application server 14 (application system) and use which received information were required It writes in addition that actual processings (for example, the contents of processing equivalent to step 220 mentioned later etc.) are greatly different with the function in which the application server 14 (application system) and use which received information were required.
[0080] At step 212, the ticket contained in the information received from the client PC 12 is extracted, and the user who is operating the client PC 12 of a requiring agency is attested based on the extracted ticket. This user authentication can be performed by judging whether it is the just ticket with which the received ticket was published by the operational administration server 16. Specifically For example, the operational administration server 16 decrypts a ticket using the public

key corresponding to the private key used for encryption. While collating whether it registers with the authority information DB the user ID contained in a series of information acquired by decryption is remembered to be by HDD30, Magic WORD contained in said a series of information can be performed by collating with the Magic WORD of normal.
[0081] In addition, the expiration date is prepared in the ticket published by the operational administration server 16. With this operation gestalt, the expiration date of a ticket is made into less than 24-hour", after a ticket is published by "operational administration server 16. The time of the ticket date of issue is included in a series of information acquired by decrypting a ticket, and at step 212, when the elapsed time from the time of the ticket date of issue judges [whether it is also less than 24 hours or] and has passed for 24 hours or more, it is judged that it is not a just ticket. In this case, once a user logs out of the MI system 10, he is logging in again, and he needs to acquire a ticket again.
[0082] At step 214, the user who is demanding use of a specific function through a client PC 12 judges whether it is the valid user which has the use authority of a corresponding application system based on the result of the authentication in step 212. When the received ticket is judged not to be the just ticket published by the operational administration server 16, the judgment of step 214 is denied, it shifts to step 230, the error response which notifies the purport which does not have the use authority of an application system for a user to correspond is returned to the client PC 12 of a requiring agency, and it returns to step 210.
[0083] Even if it can know a means for those who intend that it will use unjustly to do direct access of the function of the request which a desired application system offers to an application server 14 from a client PC 12 As mentioned above, if the just ticket is not owned, become an error, and since it is very difficult to forge a ticket By performing user authentication by the ticket by the application system side, it can prevent using the MI system 10 unjustly, without logging in to the MI system 10.
[0084] On the other hand, when the received ticket is judged to be the just ticket published by the operational administration server 16, it shifts to step 216, and the information corresponding to the user who is demanding use of a specific function is extracted by retrieving the authority information DB using the user ID contained in said a series of information. And in the following step 218, it judges whether based on the information extracted by retrieval of step 216, the user who is demanding use of a specific function has the use authority of a specific function.
[0085] For example, in the RTGS system, the pattern of use authority is defined for every its affiliation post and executive. The information for specifying whether the use authority of each user who has the use authority of a RTGS system supports which pattern Since it is matched with each user's user ID and the authority information DB on a RTGS system memorizes, the judgment of the existence of use authority For example, it is based on the user ID of the user who is demanding use of a specific function. The use authority pattern showing this user's use authority is specified, and it accomplishes by judging whether the specific functions in which use is demanded are "those with use authority" on said specified use authority pattern.
[0086] Moreover, although the pattern of use authority is created regardless of its affiliation post of a user and an executive, for example in a RAPID system The information for specifying whether the use authority of each user who has the use authority of a RAPID system supports which pattern Since it is matched with each user's user ID and the authority information DB on a RAPID system memorizes, the judgment of the existence of use authority It is based on the user ID of the user who is demanding use of a specific function like a RTGS system. The use authority pattern showing this user's use authority is specified, and it accomplishes by judging whether the specific functions in which use is demanded are "those with use authority" on said specified use authority pattern.
[0087] Furthermore, for example in a PYRAMID system, since two or more categories (refer to Table 3) exist as use authority granted to a user, the existence of use authority judges whether it is the function in which the specific function in which use is demanded from the user belongs to which category, and is judged by the judgment approach according to the judged category.

[0088] namely, about "operation authority" The use authority of the various functions belonging to "operation authority" is patternized for every operation authority class. Since the operation authority class of each user who has the use authority of a PYRAMID system is matched with user ID and memorized by the authority information DB on a PYRAMID system When it is the function in which the specific function in which use was required from the user belongs to "operation authority", the judgment of the existence of use authority For example, it is based on the user ID of the user who is demanding use of a specific function. This user's operation authority class is specified and it accomplishes by judging whether the specific functions in which use is demanded are "those with use authority" on the use authority pattern corresponding to said specified operation authority class.
[0089] moreover, about "dealings operation authority" While the use authority of the various functions belonging to "dealings operation authority" is patternized for every dealings operation authority class Their affiliation post and a management partition are set to the use authority relevant to "dealings operation authority" as a unit. Dealings operation authority class, their affiliation post, and management partition of each user who has the use authority of a PYRAMID system are matched with user ID, and are memorized by the authority information DB on a PYRAMID system.
[0090] When it is the function in which the specific function in which use was required from the user belongs to "dealings operation authority", for this reason, the judgment of the existence of use authority For example, it is based on the user ID of the user who is demanding use of a specific function. Dealings operation authority class, their affiliation post, and management partition of this user are specified respectively. The specific functions in which use is demanded are "those with use authority" on the use authority pattern corresponding to said specified dealings operation authority class. And it accomplishes by judging whether it is the inside of use authority (namely, AND of the use authority specified by the use authority, its affiliation post, and management partition which are specified by the dealings operation authority class (AND)) also by the use authority to make into a unit one's affiliation post and management partition which were specified.
[0091] When the user who is demanding use of a specific function does not have the use authority of a specific function, the judgment of step 218 is denied and it shifts to step 230, and to the client PC 12 of a requiring agency, the error response which notifies the purport which is outside a user's use authority is returned, and the specific function to in_which use was required returns to step 210.

[0092] Moreover, when the user has the use authority of the specific function in which use is demanded, the judgment of step 218 is affirmed, it shifts to step 220, and processing which offers a specific function according to a demand of a user is performed. The processing which updates the information the user instructed updating to be, the processing which perform a predetermined operation according to directions of a user, the processing which transmit predetermined information (wording of a telegram) to other computers according to directions of a user are mentioned among the processing which reads the information as which the user demanded the display on the display 54 of a client PC 12, for example from HDD 30 grade as this processing, and the information which are memorized by HDD 30 grade.
[0093] At step 222, the screen definition information for displaying the result of this processing on the display 54 of the client PC 12 of a requiring agency is generated based on the processing result performed at step 220. It judges whether the items (for example, carbon button for choosing the function in which the user does not have use authority etc.) in which the user does not have use authority are in the screen defined by the following step 224 using the screen definition information generated at step 222.
[0094] When the judgment of step 224 is affirmed, it shifts to step 226, and after changing the contents of screen definition information so that the item in which the user does not have use authority may become an inactive display like the above-mentioned MI menu screen, it shifts to

step 228. In addition, it replaces with making it an inactive display, and you may make it change the contents of screen definition information so that it may not be displayed on a display 54. Moreover, when the judgment of step 224 is denied, it shifts to step 228, without processing in any way. And at step 228, screen definition information etc. is transmitted to the client PC 12 of a requiring agency, and it returns to step 210.

[0095] If the client PC 12 which transmitted the ticket etc. receives a certain response from the application server 14 of a transmission place, the judgment of step 130 of MI system use processing (drawing 5) will be affirmed, and the response from an application server 14 will judge whether it is a normal response at the following step 132. When the response from an application server 14 is an error response, while said judgment is denied, shift to step 136 and displaying a predetermined error screen on a display 54, the message which notifies the purport whose selected application system is outside a user's use authority, or the specific function that use was required display the message notify the purport it is outside a user's use authority according to the contents of the received error response.

[0096] Moreover, when the response from an application server 14 is a normal response, the judgment of step 132 is affirmed, it shifts to step 134, and the processing result of the application server 14 (application system) to having required use for the specific function previously is displayed on a display 54 based on the screen definition information received from the application server 14. Thereby, a user can refer to or check the processing result about the specific function whose user demanded use.

[0097] At the following step 138, it judges whether use of other specific functions which an application system offers was chosen by the user. When a judgment is denied, it shifts to step 140, and it judges whether use termination of an application system was chosen by the user. Step 138,140 is repeated until return and judgment [which] are affirmed by step 138, when this judgment is also denied.

[0098] For example, a user operates a keyboard 58 and mouse 56 grade, when the specific item corresponding to a specific function to use among the items displayed on the display 54 is chosen, the judgment of step 138 will be affirmed and the processing after return and step 128 mentioned above will be repeated by step 128. Thereby, a user can carry out business, using a function (function in which self has use authority) required for execution of business, among the various functions which an application system offers. If use termination of an application system is chosen by the user, the judgment of step 140 is affirmed, return will be displayed on step 122 and MI menu screen will be again displayed on a display 54.

[0099] By the way, the carbon button 84 for changing the password other than the carbon button 82 for choosing the application system to be used and the carbon button 86 for logging out of the MI system 10 are also formed in MI menu screen (drawing 9). Moreover, although indicated by inactive in drawing 9 , the carbon button 88 for a system administrator to do a maintenance activity etc. is also formed.

[0100] It judges whether in the condition that MI menu screen is displayed on the display 54, when carbon buttons other than carbon button 82 were chosen by the user, it shifted to step 142 through step 124,126 from step 122, and the log out from the MI system 10 was chosen by the user.

[0101] When a judgment is denied, it shifts to step 150, and activation of the processing (for example, processing for changing a password and processing for a system administrator to work maintenance etc.) corresponding to the carbon button which the user chose is required of the operational administration server 16. Thereby, in the operational administration server 16, it shifts to step 198 through step 170,172 of MI operational administration processing (drawing 6), and processing according to the demand from a client PC 12 is performed. And if the processing corresponding to the carbon button which the user chose is completed, it will return from step 150 of MI system use processing (drawing 5) to step 122.

[0102] Moreover, when the carbon button 86 for logging out of the MI system 10 is chosen by the

user, it shifts to step 144 from step 142, and the ticket stored in HDD60 is discarded. At step 146, user ID is transmitted to an operational administration server, and the log out from the MI system 10 is required, and in the following step 148, it stands by until it receives a response.
[0103] In the operational administration server 16, if a log out is required from a client PC 12, it will shift to step 192 through step 170,172 of MI operational administration processing (drawing 6). User ID which received is used as a key, a log in managed table is searched with step 192, and applicable information (user ID, log in time, etc.) is deleted from a log in managed table based on the result of the retrieval in step 192 at step 194. And the response which notifies the purport which it has logged out of normally is transmitted to the client PC 12 of log out demand origin.
[0104] By this response being received by the client PC 12 of log out demand origin, the judgment of step 148 of MI system use processing (drawing 5) is affirmed, and activation of MI system use processing is completed.
[0105] Then, processing when the response of the operational administration server 16 becomes a time-out (when the judgment of step 114 of MI system use processing (drawing 5) is affirmed) is explained. Since the operational administration server 16 has doubled with this operation gestalt, when the response from the operational administration server 16 becomes a time-out, it can be judged that it is in the condition that a failure generates the both system of the operational administration server 16, and a response cannot be returned.
[0106] For this reason, when the judgment of step 114 is affirmed, it shifts to step 116, and a log in to the MI system 10 is required by transmitting the user ID and the password which were entered by the user who is demanding the log in to the server 18 for failures. At the following step 118, it judges whether the response was received from the server 18 for failures, and it stands by until a judgment is affirmed.
[0107] With this operation gestalt, since User Information DB is not formed in the server 18 for failures, if a log in is required from a client PC 12, the server 18 for failures will generate the ** ticket (ticket whose user ID is not set up) at the time of a failure, and will transmit to the client PC 12 of log in demand origin. If the ** ticket is received from the server 18 for failures at the time of a failure, the judgment of step 118 is affirmed, and the client PC 12 which required the log in from the server 18 for failures shifts to step 120, sets the user ID of the user who is demanding the log in as the ** ticket at the time of the received failure, and after storing in HDD60, it will shift to step 122.
[0108] Also when a failure occurs in the operational administration server 16 and the ticket of normal is not published by this, each application system of the MI system 10 can be used by using the ** ticket at the time of the failure published by the server 18 for failures. Moreover, also when the failure has occurred in the operational administration server 16, since the check of the use authority based on user ID is performed in each application system, a user can use the application system besides use authority, or it can prevent using the function besides use authority.
[0109] In addition, the exclusive program (MI system use program) for using the MI system 10 above is installed in the client PC 12. Although the case where use of the MI system 10 was attained was explained to the example by a client PC 12 performing MI system use processing according to this program This invention is not limited to this and this invention can be realized also under the environment where only general programs, such as a browser, are installed in the client PC 12 for example.
[0110] Moreover, the authority information DB which specifies the use authority for every user to all the application systems contained in the MI system 10 above is established. Although each application system explained the case where it was judged whether the user has the use authority of a specific function based on the authority information DB while performing user authentication using a ticket whenever use of a specific function was required from the user The application system (for example, application system which provides all users with all the functions that can be offered) with each user's fixed use authority may be contained in the computer system concerning this invention instead of what is limited to this. In this case, as for the user authentication which

used the ticket for security nature reservation, not omitting is desirable although the judgment of use authority is omissible.
[0111] Moreover, although the example which applied this invention to the computer system of a financial institution above was explained, it is not limited to this and it cannot be overemphasized that this invention can be applied to the computer system of the arbitration constituted including two or more application systems.
[0112]
[Effect of the Invention] As explained above, claim 1 and invention according to claim 9 While memorizing User Information for checking each available user for computer system, and the 1st authority information for specifying the application system with which each user has use authority for the 1st storage means For the 2nd storage means established corresponding to the application system The inside of two or more sorts of functions in which a corresponding application system can be offered, The 2nd authority information for specifying the function in which each user has use authority is memorized. Based on User Information, an user validation is performed to a log in demand of the user to computer system. Use is permitted to the user who has checked that he was a just user only about the application system with which said user has use authority based on the 1st authority information. Since an application system provides said user only with the function in which said user has use authority, to the user who is demanding use of the function with which a self-system can provide a user based on the 2nd authority information It has the outstanding effectiveness that it can realize controlling use of the system by each user according to the use authority defined for each user of every, without spoiling maintenance nature and security nature.
[0113] Invention according to claim 5 is set to invention according to claim 1. An application system Since it judges whether the user has the use authority of a function demanded whenever use of which function of two or more sorts of functions which can be offered is demanded by the user It has the effectiveness that it can prevent certainly that each function in which each application system can be offered is unjustly used by the user without use authority in addition to the above-mentioned effectiveness.
[0114] Invention according to claim 6 gives ticket information to the user who has checked that he was a just user in invention according to claim 1. Each application system Because the user who is demanding use of the function which can be offered judges whether just ticket information is possessed It has the effectiveness that it can prevent that unjust use of the computer system is carried out, without passing through the check of being a just user by check / authorization means in addition to the above-mentioned effectiveness, since said user judges whether you are a just user.
[0115] In invention according to claim 6, since invention according to claim 8 gave the user the ticket information for failures to the log in demand of the user to computer system when abnormalities arose for check / authorization means, also when abnormalities arise for check / authorization means in addition to the above-mentioned effectiveness, it has the effectiveness that a just user can avoid lapsing into the condition that no application systems can be used.

[Translation done.]

* NOTICES *

JPO and NCIPI are not responsible for any
damages caused by the use of this translation.

1.This document has been translated by computer. So the translation may not reflect the original precisely.

2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

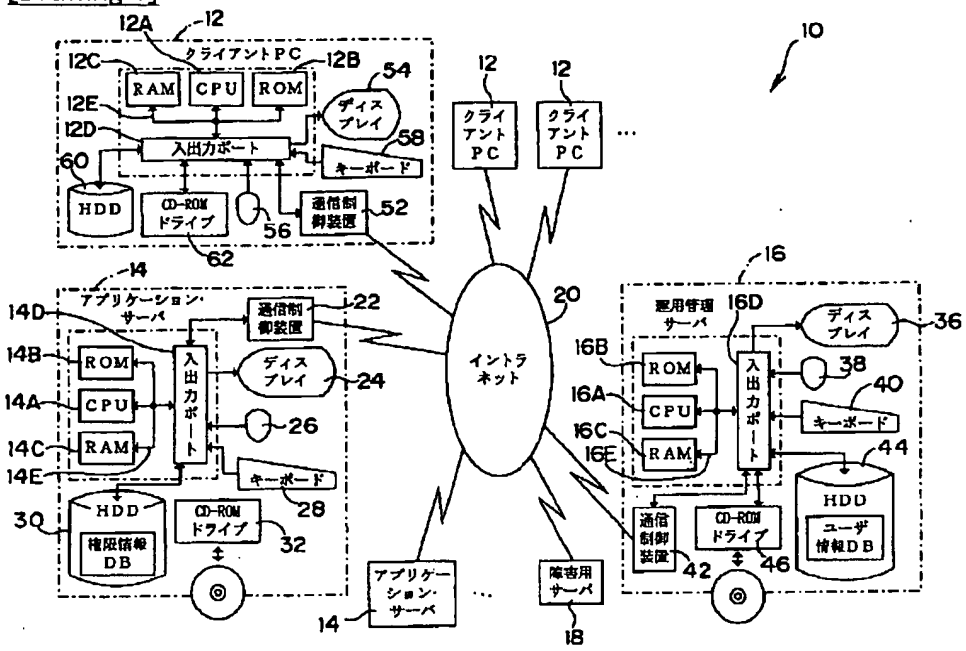
DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1] It is the block diagram showing the outline configuration of the computer system concerning this operation gestalt.
[Drawing 2] It is the image Fig. showing an example of the User Information setting screen of a RTGS system.
[Drawing 3] It is the image Fig. showing an example of the User Information setting screen of a RAPID system.
[Drawing 4] It is the image Fig. showing an example of the User Information setting screen of a RAPID system.
[Drawing 5] It is the flow chart which shows the contents of MI system use processing performed by Client PC.
[Drawing 6] It is the flow chart which shows the contents of MI operational administration processing performed by the operational administration server.
[Drawing 7] It is the flow chart which shows the contents of the MI application process performed by the application server.
[Drawing 8] It is the image Fig. showing an example of MI log in screen.
[Drawing 9] It is the image Fig. showing an example of MI menu screen.
[Drawing 10] It is the image Fig. showing an example of the menu bar of a RTGS system.
[Drawing 11] It is the image Fig. showing an example of the main menu screen of a RAPID system.
[Description of Notations]
10 Computer System
12 Client PC
14 Application Server
16 Operational Administration Server
18 Server for Failures
20 Intranet
30 HDD
44 HDD
54 Display
56 Mouse
58 Keyboard

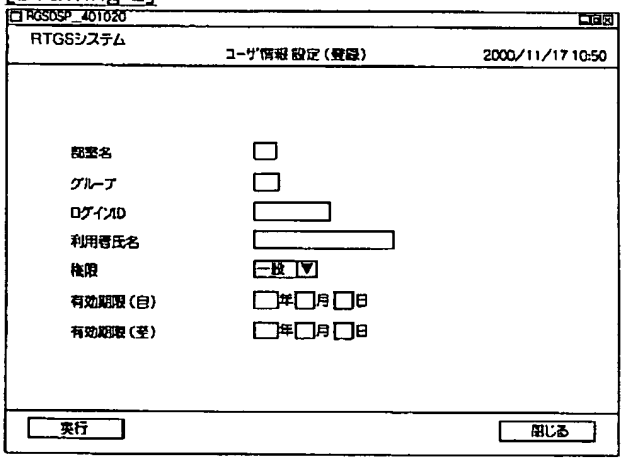
[Translation done.]

DRAWINGS

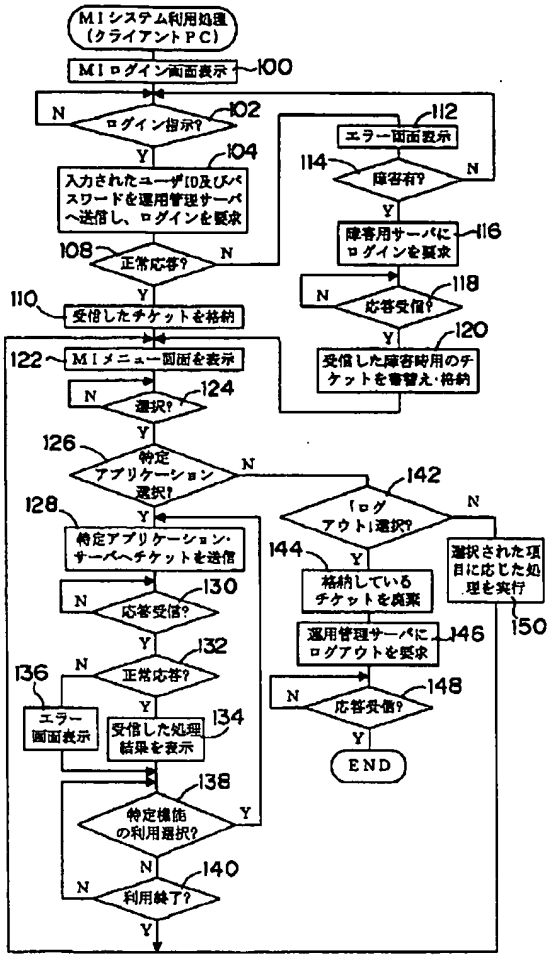
[Drawing 1]

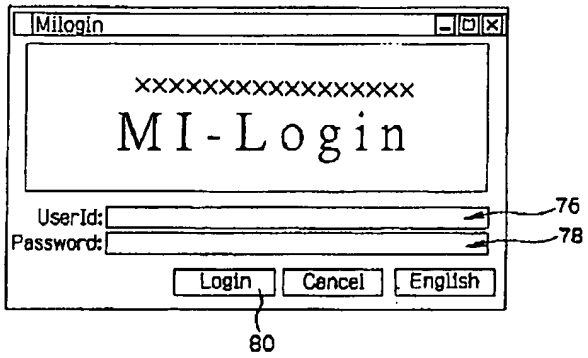


[Drawing 2]



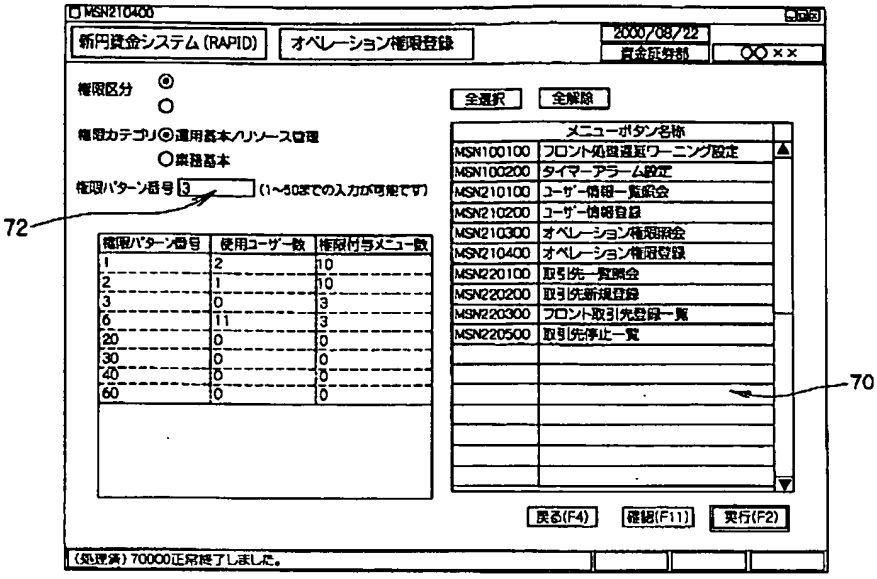
[Drawing 5]



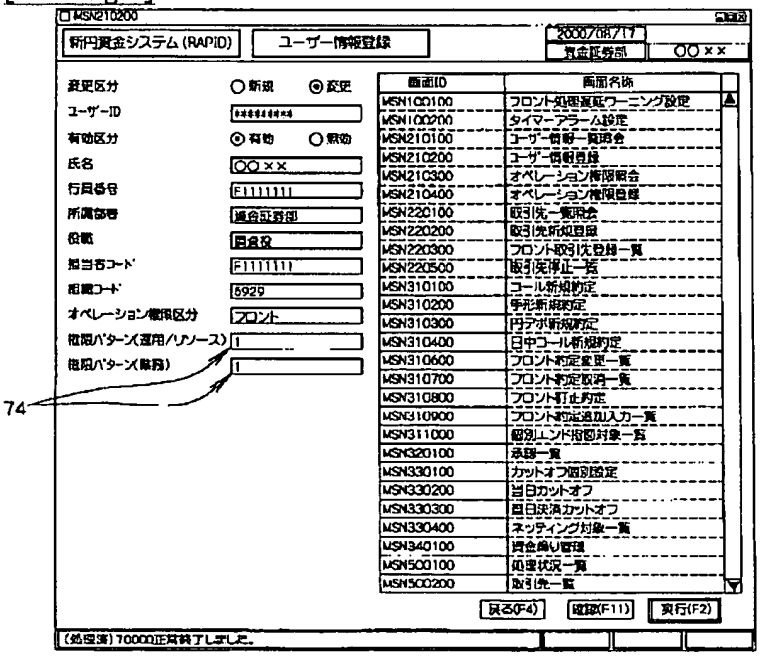


[Drawing 8]

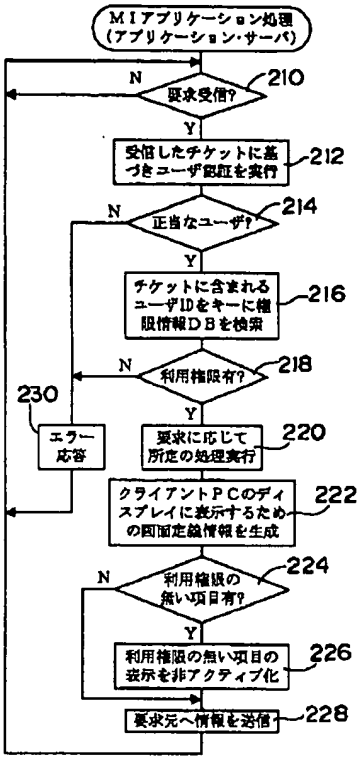
[Drawing 3]



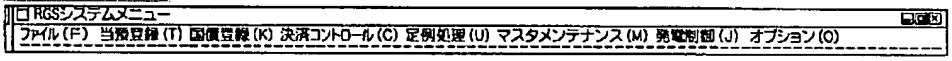
[Drawing 4]



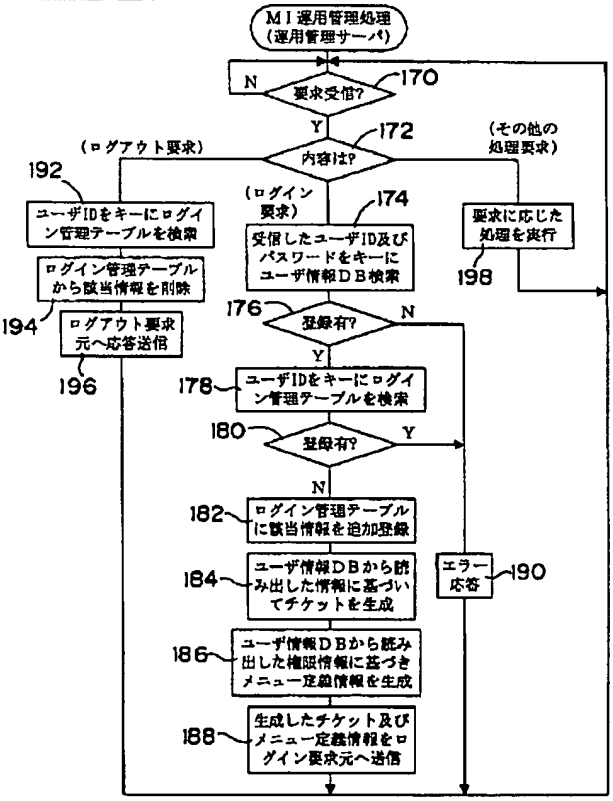
[Drawing 7]

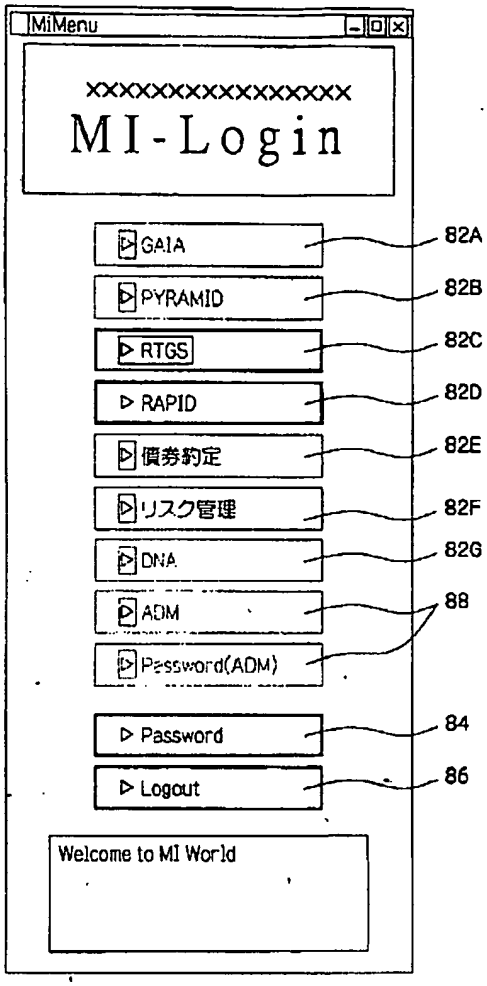


[Drawing 10]



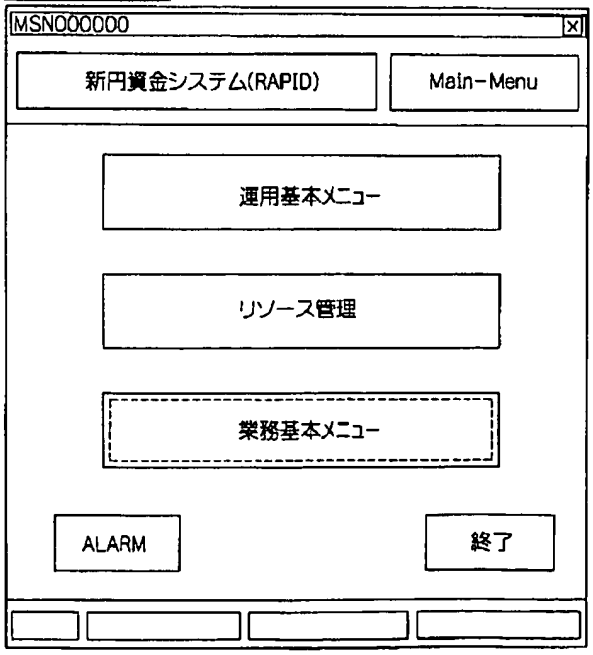
[Drawing 6]





[Drawing 9]

[Drawing 11]



[Translation done.]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2003－67336
（Ｐ２００３－６７３３６Ａ）
(43)公開日　平成15年３月７日(2003.3.7)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）
G06F 15/00	330	G06F 15/00	330 Ｂ	5B085

審査請求　有　請求項の数９　ＯＬ　（全18頁）

(21)出願番号　特願2001－255996(Ｐ2001－255996)

(22)出願日　平成13年８月27日(2001.8.27)

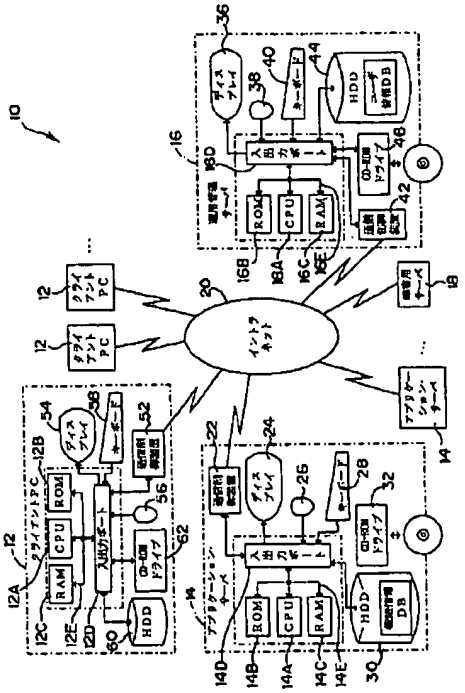
特許法第64条第２項ただし書の規定により図面第８図、９図の一部は不掲載とした。

(71)出願人　598049322
株式会社東京三菱銀行
東京都千代田区丸の内２丁目７番１号
(72)発明者　中森　行雄
東京都目黒区青葉台４－８－６　株式会社東京三菱銀行内
(72)発明者　亀田　浩樹
東京都目黒区青葉台４－８－６　株式会社東京三菱銀行内
(74)代理人　100079049
弁理士　中島　淳　（外３名）

Ｆターム(参考)　5B085 AE02 BC01 BE07 BG07 CE01

(54)【発明の名称】コンピュータ・システム及びユーザ管理方法

(57)【要約】
【課題】　個々のユーザ毎に定められた利用権限に従って個々のユーザによるシステムの利用をコントロールすることを、メインテナンス性やセキュリティ性を損なうことなく実現する。
【解決手段】　個々のサーバ14によって実現される複数のアプリケーション・システムを含むＭＩシステム10を利用するにあたり、ＰＣ12を介して運用管理サーバ16へユーザＩＤ等を送信してログインを要求すると、サーバ16はユーザＩＤのチェック後にチケットを発行し、ユーザが利用権限を有するアプリケーション・システムのみ利用可能なメニュー画面をディスプレイ54に表示させる。個々のアプリケーション・システムが提供する各種機能の利用は、対応するサーバ14へチケットを送信することで行われ、サーバ14ではチケットによるユーザ認証を行った後に、要求された機能の利用権限をユーザが有している場合にのみ要求された機能を提供する。



1

【特許請求の範囲】

【請求項１】　ユーザによって操作される端末と通信回線を介して接続されたコンピュータが、複数種のアプリケーション・プログラムを含むプログラム群を実行することで実現され、複数種のアプリケーション・システムを含んで構成されたコンピュータ・システムであって、

前記コンピュータ・システムを利用可能な個々のユーザを確認するためのユーザ情報と、前記複数種のアプリケーション・システムのうち前記個々のユーザが利用権限を有しているアプリケーション・システムを特定するための第１権限情報を記憶する第１記憶手段と、

前記複数種のアプリケーション・システムのうち、ユーザに提供可能な複数種の機能についての個々のユーザの利用権限が一定でない個々のアプリケーション・システムに対応して設けられ、対応するアプリケーション・システムがユーザに提供可能な複数種の機能のうち、前記アプリケーション・システムの利用権限を有する個々のユーザが利用権限を有している機能を特定するための第２権限情報を記憶する第２記憶手段と、

前記コンピュータ・システムへのユーザのログイン要求に対し、前記第１記憶手段に記憶されているユーザ情報に基づいてユーザの確認を行い、正当な利用者であることを確認できたユーザに対し、前記第１権限情報に基づき前記ユーザが利用権限を有しているアプリケーション・システムについてのみ利用を許可する確認・許可手段と、

を備え、

前記第２記憶手段が設けられているアプリケーション・システムは、自システムがユーザに提供可能な機能の利用を要求しているユーザに対し、対応する第２記憶手段に記憶されている第２権限情報に基づいて、前記ユーザが利用権限を有している機能のみを前記ユーザに提供することを特徴とするコンピュータ・システム。

【請求項２】　前記確認・許可手段は、ユーザが個々のアプリケーション・システムの利用を要求するためのメニュー画面に、前記正当な利用者であることを確認できたユーザが利用権限を有しているアプリケーション・システムのみを選択肢として表示させることで、前記ユーザが利用権限を有しているアプリケーション・システムについてのみ利用を許可することを特徴とする請求項１記載のコンピュータ・システム。

【請求項３】　前記第２記憶手段が設けられているアプリケーション・システムは、自システムがユーザに提供可能な機能の利用を要求しているユーザに対し、前記提供可能な機能の利用をユーザが要求するための画面に、前記ユーザが利用権限を有している機能のみを選択肢として表示させるか、又は、前記ユーザが利用権限を有していない機能の利用が前記ユーザから要求された場合に利用権限外であることを報知することで、前記ユーザが利用権限を有している機能のみを前記ユーザに提供することを特徴とする請求項１記載のコンピュータ・システム。

2

【請求項４】　前記第２権限情報は、対応するアプリケーション・システムがユーザに提供可能な機能についてのユーザの利用権限のレベルを複数のクラスに分類したときに、前記アプリケーション・システムの利用権限を有する個々のユーザが前記複数のクラスの何れに属するかを表す情報、又は、対応するアプリケーション・システムがユーザに提供可能な各機能について、前記アプリケーション・システムの利用権限を有する個々のユーザが利用権限を有するか否かを各々表す情報であることを特徴とする請求項１記載のコンピュータ・システム。

【請求項５】　前記第２記憶手段が設けられているアプリケーション・システムは、自システムがユーザに提供可能な複数種の機能のうちの何れかの機能の利用がユーザから要求される毎に、利用が要求されている機能の利用権限を前記ユーザが有しているか否かを判断することを特徴とする請求項１記載のコンピュータ・システム。

【請求項６】　前記確認・許可手段は、正当な利用者であることを確認できたユーザに対し、前記ユーザが利用権限を有するアプリケーション・システムを前記ユーザが利用する際に用いるためのチケット情報を与え、前記複数種のアプリケーション・システムの各々は、自システムがユーザに提供可能な機能の利用を要求しているユーザが正当なチケット情報を所持しているか否かを判断することで、前記利用を要求しているユーザが自システムの利用権限を有している正当な利用者か否かを判定することを特徴とする請求項１記載のコンピュータ・システム。

【請求項７】　前記確認・許可手段は、前記チケット情報として、所定の情報を秘密鍵によって暗号化した情報を用い、前記複数種のアプリケーション・システムの各々は、前記ユーザから前記端末を介して送信されたチケット情報を公開鍵によって復号化した際に前記所定の情報が再現されるか否かに基づいて、前記ユーザが正当なチケット情報を所持しているか否かを判断することを特徴とする請求項６記載のコンピュータ・システム。

【請求項８】　前記確認・許可手段に異常が生じた場合に、前記コンピュータ・システムへのユーザのログイン要求に対し、前記ユーザのユーザＩＤを付加することで前記ユーザがアプリケーション・システムを利用する際に使用可能な障害用チケット情報をユーザに与える障害チケット提供手段を更に備えたことを特徴とする請求項６記載のコンピュータ・システム。

【請求項９】　ユーザによって操作される端末と通信回線を介して接続されたコンピュータが、複数種のアプリケーション・プログラムを含むプログラム群を実行することで実現され、複数種のアプリケーション・システムを含んで構成されたコンピュータ・システムに適用可能なユーザ管理方法であって、

前記コンピュータ・システムを利用可能な個々のユーザを確認するためのユーザ情報と、前記複数種のアプリケーション・システムのうち前記個々のユーザが利用権限を有しているアプリケーション・システムを特定するための第１権限情報を第１記憶手段に記憶しておくと共に、

前記複数種のアプリケーション・システムのうち、ユーザに提供可能な複数種の機能についての個々のユーザの利用権限が一定でない個々のアプリケーション・システムに対応して設けられた第２記憶手段に、対応するアプリケーション・システムがユーザに提供可能な複数種の機能のうち、前記アプリケーション・システムの利用権限を有する個々のユーザが利用権限を有している機能を特定するための第２権限情報を記憶しておき、

前記コンピュータ・システムへのユーザのログイン要求に対し、前記第１記憶手段に記憶されているユーザ情報に基づいてユーザの確認を行い、

正当な利用者であることを確認できたユーザに対し、前記第１権限情報に基づき前記ユーザが利用権限を有しているアプリケーション・システムについてのみ利用を許可し、

前記第２記憶手段が設けられているアプリケーション・システムに対し、ユーザより前記アプリケーション・システムが提供可能な機能の利用が要求された場合に、対応する第２記憶手段に記憶されている第２権限情報に基づいて、前記ユーザが利用権限を有している機能のみを前記ユーザに提供することを特徴とするユーザ管理方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明はコンピュータ・システム及びユーザ管理方法に係り、特に、複数種のアプリケーション・システムを含んで構成されたコンピュータ・システム、及び該コンピュータ・システムに適用可能なユーザ管理方法に関する。

【０００２】

【従来の技術】コンピュータ・システムにおいて、予め登録された正当なユーザ以外の他者の不正利用を排除することは、一般に、正当なユーザのユーザ情報（例えばユーザＩＤとパスワード）を予め記憶しておき、コンピュータ・システムにログインしようとしているユーザに対してユーザ情報の送信を要求し、パーソナル・コンピュータ（ＰＣ）等の端末を介してユーザ側から送信されたユーザ情報を予め記憶されているユーザ情報と照合し、ログインしようとしているユーザが正当なユーザか否かを判断することによって行われる。コンピュータ・システムが提供する機能（サービス）は、正当なユーザであると判断されて正常にログインできたユーザのみが利用可能となる。

【０００３】また、コンピュータ・システムが提供する種々の機能の中には、正当なユーザのうちの一部のユーザに対してのみ利用を許可している機能が存在している場合もある。このような場合、コンピュータ・システムは、提供機能に対する個々のユーザの利用権限を規定する権限情報を予め記憶しておき、ログインしたユーザの権限情報を参照し、ログインした個々のユーザに対して個々のユーザが利用権限を有している機能のみを提供するように構成される。なお、権限情報はユーザ情報と共に単一のデータベース（ＤＢ）に保存されることが一般的であった。

【０００４】

【発明が解決しようとする課題】ところで、金融機関では、業務の効率向上・顧客へのサービス向上を目的として、かなり以前より業務の機械化に取り組んでいるが、金融機関における業務は多種多様であるために、互いに異なる業務の遂行を支援するための互いに独立した多数種のアプリケーション・システムが存在しており、各アプリケーション・システムを利用するためには、個々のアプリケーション・システム毎に設けられた専用端末を操作して各アプリケーション・システムに個別にログインする必要があった。このため、各種のアプリケーション・システムを統合して単一のコンピュータ・システムを構築することが検討されている。

【０００５】しかしながら、上記のように互いに異なるサービスを提供する複数種のアプリケーション・システムを統合して単一のコンピュータ・システムを構築した等の場合、例えば或るアプリケーション・システムの権限情報が、ユーザの利用権限のレベルを複数のクラスに分類したときに個々のユーザが何れのクラスの何れに属するかを表す情報であるのに対し、別のアプリケーション・システムの権限情報は、アプリケーション・プログラムがユーザに提供可能な全機能について個々のユーザが利用権限を有するか否かを各々規定する情報である等のように、権限情報の体系自体からして個々のアプリケーション・システム毎に相違していることが多い。

【０００６】このような場合に、個々のアプリケーション・システムに対応する権限情報を統合し、ユーザ情報と共に単一のＤＢに保存したとすると、ＤＢに保存する情報のデータ構造が極めて複雑になるので、例えばユーザの新規追加、或いは特定のアプリケーション・システムに対応する権限情報のデータ構造の変更（例えば利用権限のレベルを分類するクラス数の変更や、個々のユーザの利用権限を詳細に定めたテーブルの追加等）を行う必要が生じた場合の作業が非常に煩雑となり、メインテナンス性が大幅に低下するという問題がある。

【０００７】また、上記のように、個々のユーザを単位としてコンピュータ・システムの利用を管理するための情報（各アプリケーション・システムに対応する権限情報やユーザ情報）をＤＢに一元管理すると、正当なユーザ以外の他者が、コンピュータ・システムに侵入して上

5

記のＤＢに保管されている情報を書き替えることで、コンピュータ・システムを自由に不正利用することも可能となってしまうため、セキュリティの面からも好ましくない。

【０００８】本発明は上記事実を考慮して成されたもので、個々のユーザ毎に定められた利用権限に従って個々のユーザによるシステムの利用をコントロールすることを、メインテナンス性やセキュリティ性を損なうことなく実現できるコンピュータ・システム及びユーザ管理方法を得ることが目的である。

【０００９】

【課題を解決するための手段】上記目的を達成するために請求項１記載の発明に係るコンピュータ・システムは、ユーザによって操作される端末と通信回線を介して接続されたコンピュータが、複数種のアプリケーション・プログラムを含むプログラム群を実行することで実現され、複数種のアプリケーション・システムを含んで構成されたコンピュータ・システムであって、前記コンピュータ・システムを利用可能な個々のユーザを確認するためのユーザ情報と、前記複数種のアプリケーション・システムのうち前記個々のユーザが利用権限を有しているアプリケーション・システムを特定するための第１権限情報を記憶する第１記憶手段と、前記複数種のアプリケーション・システムのうち、ユーザに提供可能な複数種の機能についての個々のユーザの利用権限が一定でない個々のアプリケーション・システムに対応して設けられ、対応するアプリケーション・システムがユーザに提供可能な複数種の機能のうち、前記アプリケーション・システムの利用権限を有する個々のユーザが利用権限を有している機能を特定するための第２権限情報を記憶する第２記憶手段と、前記コンピュータ・システムへのユーザのログイン要求に対し、前記第１記憶手段に記憶されているユーザ情報に基づいてユーザの確認を行い、正当な利用者であることを確認できたユーザに対し、前記第１権限情報に基づき前記ユーザが利用権限を有しているアプリケーション・システムについてのみ利用を許可する確認・許可手段と、を備え、前記第２記憶手段が設けられているアプリケーション・システムは、自システムがユーザに提供可能な機能の利用を要求しているユーザに対し、対応する第２記憶手段に記憶されている第２権限情報に基づいて、前記ユーザが利用権限を有している機能のみを前記ユーザに提供することを特徴としている。

【００１０】請求項１記載の発明に係るコンピュータ・システムは、ユーザによって操作される端末（ＰＣ等から成るクライアント・コンピュータであってもよいし、ＴＳＳ端末装置等の端末であってもよい）と通信回線を介して接続されたコンピュータが、複数種のアプリケーション・プログラムを含むプログラム群を実行することで実現され、複数種のアプリケーション・システム（コンピュータが各アプリケーション・プログラムを実行することで実現されるシステム）を含んで構成されている。なお、前記プログラム群を実行するコンピュータは単一のコンピュータであってもよいが、複数台のコンピュータで前記プログラム群を分担して実行する構成の方が、コンピュータに加わる負荷を分散させることができるので好ましい。

6

【００１１】請求項１記載の発明では、コンピュータ・システムを利用可能な個々のユーザを確認するためのユーザ情報、及び複数種のアプリケーション・システムのうち個々のユーザが利用権限を有しているアプリケーション・システムを特定するための第１権限情報が第１記憶手段に記憶されており、確認・許可手段は、コンピュータ・システムへのユーザのログイン要求に対し、第１記憶手段に記憶されているユーザ情報に基づいてユーザの確認を行い、正当な利用者であることを確認できたユーザに対し、第１権限情報に基づきユーザが利用権限を有しているアプリケーション・システムについてのみ利用を許可する。

【００１２】なお、ユーザ情報としては、例えばユーザＩＤとパスワード等の情報を適用することができる。また、ユーザが利用権限を有しているアプリケーション・システムについてのみ利用を許可することは、例えば請求項２に記載したように、ユーザが個々のアプリケーション・システムの利用を要求するためのメニュー画面に、正当な利用者であることを確認できたユーザが利用権限を有しているアプリケーション・システムのみを選択肢として表示させることによって実現できるが、他の方法を用いてもよい。

【００１３】第１権限情報は個々のアプリケーション・システムを単位とする個々のユーザの利用権限を表す情報であり、ユーザ情報についても個々のユーザを単位とする情報であるので、第１記憶手段に記憶されるこれらの情報のデータ構造は何れも簡単である。従って、本発明に係るコンピュータ・システムを利用可能なユーザを新規追加したり、或いはアプリケーション・システムを新規追加する等を目的とした情報の書き替えも容易であり、メインテナンス性に優れている。

【００１４】また請求項１記載の発明では、複数種のアプリケーション・システムのうち、ユーザに提供可能な複数種の機能についての個々のユーザの利用権限が一定でない個々のアプリケーション・システムに対応して第２記憶手段が設けられており、この第２記憶手段には、対応するアプリケーション・システムがユーザに提供可能な複数種の機能のうち、前記アプリケーション・システムの利用権限を有する個々のユーザが利用権限を有している機能を特定するための第２権限情報が記憶されている。そして、第２記憶手段が設けられているアプリケーション・システムは、自システムがユーザに提供可能な機能の利用を要求しているユーザに対し、対応する第

２記憶手段に記憶されている第２権限情報に基づいて、前記ユーザが利用権限を有している機能のみを前記ユーザに提供する。これにより、個々のユーザ毎に定められた利用権限（第１権限情報及び第２権限情報によって規定される利用権限）に従って、個々のユーザによるシステムの利用をコントロールすることができる。

【００１５】なお、第２記憶手段が設けられているアプリケーション・システムが、自システムがユーザに提供可能な機能の利用を要求しているユーザに対し、該ユーザが利用権限を有している機能のみをユーザに提供することは、例えば請求項３に記載したように、前記ユーザに対し、前記提供可能な機能の利用をユーザが要求するための画面に、前記ユーザが利用権限を有している機能のみを選択肢として表示させるか、又は、前記ユーザが利用権限を有していない機能の利用が前記ユーザから要求された場合に利用権限外であることを報知することによって実現できるが、他の方法を用いてもよい。

【００１６】第２権限情報は、ユーザに提供可能な複数種の機能についての個々のユーザの利用権限が一定でない個々のアプリケーション・システム固有の権限情報であるので、アプリケーション・システムが提供する機能の種類等に応じて情報の体系が相違することになり、例えば請求項４に記載したように、対応するアプリケーション・システムがユーザに提供可能な機能についてのユーザの利用権限のレベルを複数のクラスに分類したときに、前記アプリケーション・システムの利用権限を有する個々のユーザが前記複数のクラスの何れに属するかを表す情報である場合もあれば、対応するアプリケーション・システムがユーザに提供可能な全機能について、前記アプリケーション・システムの利用権限を有する個々のユーザが利用権限を有するか否かを各々表す情報である場合もある。

【００１７】これに対して請求項１記載の発明では、ユーザに提供可能な複数種の機能についての個々のユーザの利用権限が一定でないアプリケーション・システムの各々に対応して第２記憶手段が設けられているので、個々の第２記憶手段に記憶されている第２権限情報は、全てのアプリケーション・システムの第２権限情報を統合した場合と比較して、データ構造が簡単になる。従って、特定のアプリケーション・システムに対応する第２権限情報の情報体系を変更する等を目的とした第２権限情報の書き替えも容易であり、メインテナンス性に優れている。

【００１８】また、請求項１記載の発明において、特定のアプリケーション・システムが提供する特定の機能を特定ユーザが利用することは、第１記憶手段に記憶されている第１権限情報が、前記特定ユーザが前記特定のアプリケーション・システムの利用権限を有していることを表す内容となっており、かつ前記特定のアプリケーション・システムに対応する第２記憶手段に記憶されている第２権限情報が、前記特定ユーザが前記特定の機能の利用権限を有していることを表す内容となっていることで初めて可能になる。このように、請求項１記載の発明では、個々のユーザの利用権限を規定する情報が第１記憶手段と第２記憶手段に分散されて管理されているので、セキュリティ性にも優れている。

【００１９】従って、請求項１記載の発明によれば、個々のユーザ毎に定められた利用権限に従って個々のユーザによるシステムの利用をコントロールすることを、メインテナンス性やセキュリティ性を損なうことなく実現することができる。

【００２０】請求項５記載の発明は、請求項１記載の発明において、第２記憶手段が設けられているアプリケーション・システムは、自システムがユーザに提供可能な複数種の機能のうちの何れかの機能の利用がユーザから要求される毎に、利用が要求されている機能の利用権限をユーザが有しているか否かを判断することを特徴としている。

【００２１】請求項５記載の発明では、第２記憶手段が設けられているアプリケーション・システムが、提供可能な複数種の機能のうちの何れかの機能の利用がユーザから要求される毎に、利用が要求されている機能の利用権限を前記ユーザが有しているか否かを判断するので、アプリケーション・システムが提供可能な機能に対するユーザの利用権限を、各アプリケーション・システムが提供可能な個々の機能を単位として管理することが可能となり、各アプリケーション・システムが提供可能な個々の機能が、利用権限のないユーザによって不正に利用されることを確実に阻止することができる。

【００２２】請求項６記載の発明は、請求項１記載の発明において、前記確認・許可手段は、正当な利用者であることを確認できたユーザに対し、前記ユーザが利用権限を有するアプリケーション・システムを前記ユーザが利用する際に用いるためのチケット情報を与え、前記複数種のアプリケーション・システムの各々は、自システムがユーザに提供可能な機能の利用を要求しているユーザが正当なチケット情報を所持しているか否かを判断することで、前記利用を要求しているユーザが自システムの利用権限を有している正当な利用者か否かを判定することを特徴としている。

【００２３】請求項６記載の発明では、正当な利用者であることを確認できたユーザにチケット情報を与え、複数種のアプリケーション・システムの各々は、ユーザが正当なチケット情報を所持しているか否かを判断することで、前記ユーザが正当な利用者か否かを判定するので、正当なチケット情報を所持していないユーザが、利用権限を有していない特定のアプリケーション・システムに直接アクセスし、該特定のアプリケーション・システムが提供する機能を不正に利用しようとした場合にも、これを阻止することができる。従って、請求項６記

載の発明によれば、確認・許可手段による正当な利用者であることの確認を経ることなく、コンピュータ・システムが不正利用されることを阻止することができる。

【００２４】なお、請求項６記載の発明において、確認・許可手段は、例えば請求項７に記載したように、チケット情報として、所定の情報を秘密鍵によって暗号化した情報を用いることができる。この場合、複数種のアプリケーション・システムの各々は、ユーザから端末を介して送信されたチケット情報を公開鍵によって復号化した際に所定の情報が再現されるか否かに基づいて、ユーザが正当なチケット情報を所持しているか否かを判断することができる。

【００２５】請求項８記載の発明は、請求項６記載の発明において、確認・許可手段に異常が生じた場合に、コンピュータ・システムへのユーザのログイン要求に対し、前記ユーザのユーザＩＤを付加することで、前記ユーザがアプリケーション・システムを利用する際に使用可能な障害用チケット情報をユーザに与える障害チケット提供手段を更に備えたことを特徴としている。

【００２６】本発明において、確認・許可手段として機能するコンピュータに何らかの異常が発生した等の理由により確認・許可手段に異常が生じ、コンピュータ・システムへのログイン要求が正常に受付けされなくなった場合、各アプリケーション・システム自体は利用可能な状態であっても、正当な利用者が全てのアプリケーション・システムを利用できない状態に陥る、という不都合がある。これに対して請求項８記載の発明では、確認・許可手段に異常が生じた場合に、障害チケット提供手段によって障害用チケット情報がユーザに与えられるので、確認・許可手段に異常が生じた場合にも、正当な利用者が全てのアプリケーション・システムを利用できない状態に陥ることを回避することができる。

【００２７】請求項９記載の発明に係るユーザ管理方法は、ユーザによって操作される端末と通信回線を介して接続されたコンピュータが、複数種のアプリケーション・プログラムを含むプログラム群を実行することで実現され、複数種のアプリケーション・システムを含んで構成されたコンピュータ・システムに適用可能なユーザ管理方法であって、前記コンピュータ・システムを利用可能な個々のユーザを確認するためのユーザ情報と、前記複数種のアプリケーション・システムのうち前記個々のユーザが利用権限を有しているアプリケーション・システムを特定するための第１権限情報を第１記憶手段に記憶しておくと共に、前記複数種のアプリケーション・システムのうち、ユーザに提供可能な複数種の機能についての個々のユーザの利用権限が一定でない個々のアプリケーション・システムに対応して設けられた第２記憶手段に、対応するアプリケーション・システムがユーザに提供可能な複数種の機能のうち、前記アプリケーション・システムの利用権限を有する個々のユーザが利用権限を有している機能を特定するための第２権限情報を記憶しておき、前記コンピュータ・システムへのユーザのログイン要求に対し、前記第１記憶手段に記憶されているユーザ情報に基づいてユーザの確認を行い、正当な利用者であることを確認できたユーザに対し、前記第１権限情報に基づき前記ユーザが利用権限を有しているアプリケーション・システムについてのみ利用を許可し、前記第２記憶手段が設けられているアプリケーション・システムに対し、ユーザより前記アプリケーション・システムが提供可能な機能の利用が要求された場合に、対応する第２記憶手段に記憶されている第２権限情報に基づいて、前記ユーザが利用権限を有している機能のみを前記ユーザに提供することを特徴としているので、請求項１記載の発明と同様に、個々のユーザ毎に定められた利用権限に従って個々のユーザによるシステムの利用をコントロールすることを、メインテナンス性やセキュリティ性を損なうことなく実現できる。

【００２８】

【発明の実施の形態】以下、図面を参照して本発明の実施形態の一例を詳細に説明する。図１には、金融機関の各種業務を支援するために金融機関に設置されたコンピュータ・システム１０（以下、ＭＩシステム１０と称する）が示されている。

【００２９】ＭＩシステム１０は、金融機関の各部署に設置された多数台のクライアントＰＣ１２（本発明の端末に相当）と、複数台のアプリケーション・サーバ１４と、運用管理サーバ１６と、障害用サーバ１８が、イントラネット２０を介して相互に接続されて構成されている。なお、アプリケーション・サーバ１４、運用管理サーバ１６及び障害用サーバ１８は、請求項１に記載のコンピュータに各々対応している。

【００３０】各アプリケーション・サーバ１４は、各々ワークステーション又は汎用の大型コンピュータから成り、ＣＰＵ１４Ａ、ＲＯＭ１４Ｂ、ＲＡＭ１４Ｃ、入出力ポート１４Ｄを備え、これらがアドレスバス、データバス、制御バス等のバス１４Ｅを介して互いに接続されて構成されている。入出力ポート１４Ｄには、各種の入出力機器として、イントラネット２０に接続された通信制御装置（例えばルータ）２２、ディスプレイ２４、マウス２６、キーボード２８、ＨＤＤ３０、及びＣＤ－ＲＯＭからの情報の読み出しを行うＣＤ－ＲＯＭドライブ３２が各々接続されている。

【００３１】金融機関では、業務の効率向上・顧客へのサービス向上を目的として、かなり以前より業務の機械化に取り組んでいるが、金融機関における業務は多種多様であるために、互いに異なる業務を支援するための互いに独立した複数種のアプリケーション・システムが存在していた。各アプリケーション・サーバ１４は、元々は個々のアプリケーション・システムを実現するために、個々のアプリケーション・システムに対応して設け

られたコンピュータであり、各アプリケーション・サーバ１４のＨＤＤ３０には、対応する特定業務を支援する処理（アプリケーション処理）をＣＰＵ１４Ａによって実行するための互いに異なるアプリケーション・プログラムが予めインストールされている。

【００３２】本実施形態に係るＭＩシステム１０は、各アプリケーション・サーバ１４によって実現される複数種のアプリケーション・システムを統合することで構築されたシステムであり、ＭＩシステム１０のユーザは、イントラネット２０に接続された単一のクライアントＰＣ１２を介してＭＩシステム１０にログインすることで、任意のアプリケーション・システムが提供する任意の機能を利用することも可能に構成されている。

【００３３】但し、ＭＩシステム１０では、各アプリケーション・システムがユーザに提供可能な各機能のうち、個々のユーザの業務に必要な機能についてのみ個々のユーザに利用権限を与えている。具体的には、ＭＩシステム１０への個々のユーザのログインの管理、及び、ＭＩシステム１０が提供可能な各機能についての個々のユーザの利用権限の管理の一部（個々のアプリケーション・システムを単位とする個々のユーザの利用権限の管理）は運用管理サーバ１６によって行われる。なお、個々のアプリケーション・システムの利用に際してのより細かな利用権限の管理は個々のアプリケーション・システム（個々のアプリケーション・サーバ１４）で行われる。

【００３４】運用管理サーバ１６はワークステーション又は汎用の大型コンピュータから成り、ＣＰＵ１６Ａ、ＲＯＭ１６Ｂ、ＲＡＭ１６Ｃ、入出力ポート１６Ｄを備え、これらがアドレスバス、データバス、制御バス等のバス１６Ｅを介して互いに接続されて構成されている。入出力ポート１６Ｄには、各種の入出力機器として、ディスプレイ３６、マウス３８、キーボード４０、イントラネット２０に接続された通信制御装置（例えばルータ）４２、ＨＤＤ４４、及びＣＤ－ＲＯＭからの情報の読み出しを行うＣＤ－ＲＯＭドライブ４６が各々接続されている。運用管理サーバ１６には、ＭＩ運用管理処理（詳細は後述）を運用管理サーバ１６のＣＰＵ１６Ａによって実行するためのＭＩ運用管理プログラムがＨＤＤ４４にインストールされている。

【００３５】障害用サーバ１８は、運用管理サーバ１６と同様にワークステーション又は汎用の大型コンピュータから成るコンピュータであり、運用管理サーバ１６に障害が発生し、ＭＩシステム１０へのログインが困難となった場合に、ユーザがＭＩシステム１０にログインするための処理を運用管理サーバ１６に代って行う。

【００３６】また、クライアントＰＣ１２はパーソナル・コンピュータ（ＰＣ）から成り、ＣＰＵ１２Ａ、ＲＯＭ１２Ｂ、ＲＡＭ１２Ｃ、入出力ポート１２Ｄを備え、これらがアドレスバス、データバス、制御バス等のバス１２Ｅを介して互いに接続されて構成されている。入出力ポート１２Ｄには、各種の入出力機器として、イントラネット２０に接続された通信制御装置（例えばルータ）５２、ディスプレイ５４、マウス５６、キーボード５８、ＨＤＤ６０、及びＣＤ－ＲＯＭからの情報の読み出しを行うＣＤ－ＲＯＭドライブ６２が各々接続されている。クライアントＰＣ１２には、ＭＩシステム利用処理（詳細は後述）をクライアントＰＣ１２のＣＰＵ１２Ａによって実行するためのＭＩシステム利用プログラムがＨＤＤ６０にインストールされている。

【００３７】次に本実施形態の作用として、まず権限情報の登録について説明する。運用管理サーバ１６のＨＤＤ４４には、ＭＩシステム１０への個々のユーザのログインの管理及び個々のアプリケーション・システムを単位とする個々のユーザの利用権限の管理を行うためのユーザ情報データベース（ＤＢ）が記憶されている。このユーザ情報ＤＢには、個々のユーザについて、例えば次の表１に示すような情報が記憶されている。

【００３８】

【表１】

＜ユーザ情報ＤＢの内容(一例)＞

項目	内容
ユーザＩＤ	xxxxxxxx
パスワード	yyyyyyyy
所属部署ＩＤ	zzzz
役職ＩＤ	wwww
その他の属性情報	vvvv
利用権限を有するアプリケーション	アプリＡ
	アプリＢ
	：

【００３９】表１において、「ユーザＩＤ」はＭＩシステム１０の利用権限を有する個々のユーザを識別するための情報であり、「パスワード」はログインに際してユーザ認証に用いる情報、「所属部署ＩＤ」「役職ＩＤ」及び「その他の属性情報」は個々のユーザの所属部署、役職やその他（例えば個々のユーザが行う業務の管理区分等）を識別するための情報である。また、本実施形態に係るＭＩシステム１０では、個々のユーザに対し、個々のユーザの業務の遂行に必要なアプリケーション・システムについてのみ利用権限を与えている。このため「利用権限を有するアプリケーション」には、個々のユーザが利用権限を有しているアプリケーション・システムのＩＤが登録設定される。ユーザ情報ＤＢへの個々のユーザの情報の登録は、ＭＩシステム１０全体を管理している部署で行われる。

【００４０】なお、上述した各種の情報のうち、「利用権限を有するアプリケーション」は本発明の第１権限情報に、それ以外の情報は本発明のユーザ情報に各々対応しており、ユーザ情報ＤＢを記憶するＨＤＤ４４は本発

13

明の第１記憶手段に対応している。表１からも明らかなように、ユーザ情報ＤＢにはアプリケーション・システムを単位とする各ユーザの利用権限のみが記憶されているので、ユーザ情報ＤＢに記憶されている情報はデータ構造が非常に簡単であり、利用ユーザを追加したり、新たなアプリケーション・システムが追加された場合に情報を更新する等のメインテナンスを簡単に行うことができる。

【００４１】また、各アプリケーション・サーバ１４のＨＤＤ３０には、個々のユーザが対応するアプリケーション・システムを利用するに際し、より細かな利用権限の管理を行うために、個々のユーザの利用権限を特定するための情報が登録された権限情報ＤＢが記憶されている。なお、権限情報ＤＢは本発明の第２権限情報に対応しており、権限情報ＤＢを記憶する各アプリケーション・サーバ１４のＨＤＤ３０は本発明の第２記憶手段に対応している。この権限情報ＤＢの内容（利用権限を規定する情報の体系）は個々のアプリケーション・システム（個々のアプリケーション・サーバ１４）によって相違している。

【００４２】すなわち、本実施形態では、各アプリケーション・サーバ１４によって実現される各アプリケーション・システムの中に、日本銀行の当座預金や国債の決済に関する業務を支援するためのアプリケーション・システム（以下、ＲＴＧＳシステムという）が含まれている。このＲＴＧＳシステムでは、例として次の表２に示すように、ユーザに与える利用権限が２次元のマトリックスを用いてユーザの所属部署及び役職毎に予めパターン化されており、所属部署及び役職毎に定められた利用権限のパターンは権限パターン情報としてＲＴＧＳシステムの権限情報ＤＢに記憶されている。

【００４３】

【表２】

〈 ＲＴＧＳシステムにおける利用権限のパターン 〉

	部署Ａ		部署Ｂ		…
	役職Ａ	役職Ｂ	役職Ａ	役職Ｂ	…
機能ａ		○		○	…
機能ｂ	○	○		●	…
機能ｃ	●	○	○	○	…
：	：	：	：	：	：

【００４４】但し、「●」は参照のみ可、「○」は参照及び更新可

従って、ＲＴＧＳシステムでは所属部署及び役職が同一のユーザに同一の利用権限が与えられるので、ＲＴＧＳシステムを利用する個々のユーザに対する利用権限の設定は、図２に例として示すユーザ情報設定画面からも明

14

らかなように、所属部署（図２では「部室名」及び「グループ」）、役職（図２では「権限」）、ユーザＩＤ（ログインＩＤ）等の情報を入力することで完了し、ＲＴＧＳシステムの権限情報ＤＢには、個々のユーザの利用権限が何れのパターンに対応しているかを特定するための情報（例えば所属部署ＩＤと役職ＩＤ等）がユーザＩＤと対応されて記憶される。

【００４５】また、ＭＩシステム１０の各アプリケーション・システムの中には、円資金に関する業務を支援するためのアプリケーション・システム（以下、ＲＡＰＩＤシステムという）が含まれている。このＲＡＰＩＤシステムでは、ユーザの所属部署及び役職と無関係に、利用権限のパターンを任意に作成可能とされている。

【００４６】すなわち、例として図３に示すＲＡＰＩＤシステムの権限パターン設定画面は、画面右側に機能名称表示欄７０が設けられており、この機能名称表示欄７０に一覧表示された機能の中から特定の機能を選択することで、選択した機能の利用権限が作成中の利用権限のパターンに付加される。作成された利用権限のパターンは、権限パターン設定画面の左側に設けられたパターン番号入力欄７２に設定されたパターン番号がＩＤとして付加され、権限パターン情報としてＲＡＰＩＤシステムの権限情報ＤＢに記憶される。

【００４７】そして、ＲＡＰＩＤシステムを利用する個々のユーザに対する利用権限の設定は、例として図４に示すユーザ情報設定画面からも明らかなように、ユーザＩＤや所属部署、役職等の情報に加え、該ユーザに設定する利用権限のパターンを設定欄７４にパターン番号（ＩＤ）で設定することで完了し、ＲＡＰＩＤシステムの権限情報ＤＢには、個々のユーザの利用権限が何れのパターンに対応しているかを特定するためのパターンＩＤ等の情報がユーザＩＤと対応されて記憶される。なお、ＲＡＰＩＤシステムでは利用権限のパターンをユーザの所属部署及び役職と無関係に作成できるので、必要に応じて個々のユーザ毎にパターンを作成することも可能であり、個々のユーザの利用権限をより細かく設定することができる。

【００４８】また、各アプリケーション・システムの中には、デリバティブに関する業務を支援するためのアプリケーション・システム（以下、ＰＹＲＡＭＩＤシステムという）が含まれている。このＰＹＲＡＭＩＤシステムでは、ユーザに与える利用権限として、次の表３に示すような複数のカテゴリが存在しており、利用権限の規定方法は各カテゴリ毎に相違している。

【００４９】

【表３】

15　　16

権限の種類	権限の内容
オペレーション権限	各種オペレーション画面を操作する権限
取引オペレーション権限	約定データに対するオペレーション権限
マーケットデータオペレーション権限	マーケットデータを登録/更新する権限
：	：

【００５０】例えば表３に示した各カテゴリのうち、「オペレーション権限」については、アシスタント／ディーラー／チーフの各役職に対応する３つのオペレーション権限クラスについて、「オペレーション権限」に属する各種機能の利用権限が各々パターン化されており、個々のオペレーション権限クラス毎の各種機能の利用権限のパターンは、オペレーション権限パターン情報としてＰＹＲＡＭＩＤシステムの権限情報ＤＢに記憶されている。

【００５１】ＰＹＲＡＭＩＤシステムを利用する個々のユーザに対する「オペレーション権限」に関する利用権限の設定は、個々のユーザが３つのオペレーション権限クラスのうちの何れのクラスに属するかを指定することによって行われ、指定したオペレーション権限クラスがユーザＩＤと対応されてＰＹＲＡＭＩＤシステムの権限情報ＤＢに記憶されることにより、個々のユーザの「オペレーション権限」に属する各種機能の利用権限（各種オペレーション画面を操作（参照のみ／参照及び更新）する権限）が登録される。

【００５２】また「取引オペレーション権限」については、アシスタント／ディーラー／チーフの各役職に対応する３つの取引オペレーション権限クラスについて、「取引オペレーション権限」に属する各種機能の利用権限が各々パターン化されていると共に、「取引オペレーション権限」に関連する利用権限（例えば取扱可能な通貨権限や取扱可能な商品権限等）が、所属部署及び個々のユーザが行う業務の管理区分を単位として定められており、個々の取引オペレーション権限クラス毎の利用権限のパターン、所属部署及び管理区分を単位とする利用権限は、取引オペレーション権限情報としてＰＹＲＡＭＩＤシステムの権限情報ＤＢに記憶されている。

【００５３】このため「取引オペレーション権限」に関しては、ＰＹＲＡＭＩＤシステムを利用する個々のユーザが３つの取引オペレーション権限クラスのうちの何れのクラスに属するかを指定すると共に、所属部署及び管理区分を指定することによって行われ、指定した取引オペレーション権限クラス、所属部署及び管理区分がユーザＩＤと対応されてＰＹＲＡＭＩＤシステムの権限情報ＤＢに記憶されることにより、個々のユーザの「取引オペレーション権限」に属する各種の利用権限（約定データに対する各種のオペレーション権限）が登録される。

【００５４】このように、各アプリケーション・システムが提供可能な各種機能を単位とする各ユーザの細かな利用権限については、対応する各アプリケーション・サーバ１４のＨＤＤ３０に記憶され、アプリケーション・システム毎に分離されているので、ＭＩシステム１０に関する各ユーザの利用権限を一元管理する場合と比較して、利用権限を規定する情報（各アプリケーション・サーバ１４の権限情報ＤＢに記憶する情報）のデータ構造が簡単になると共に、他のアプリケーション・システムの影響を受けることなく利用権限を規定する情報の体系を自由に定めることができる。従って、利用ユーザの追加等のメインテナンスや利用権限を規定する情報の体系そのものの変更等も比較的簡単に行うことができる。

【００５５】続いて図５～図７のフローチャートを参照し、ユーザがＭＩシステム１０を利用する際に各コンピュータで実行される処理について説明する。ユーザがクライアントＰＣ１２に対してＭＩシステム１０の利用を指示すると、ＭＩシステム利用プログラムがクライアントＰＣ１２のＣＰＵ１２Ａによって実行されることにより、図５に示すＭＩシステム利用処理がクライアントＰＣ１２で実行される。

【００５６】このＭＩシステム利用処理では、まずステップ１００において、例として図８に示すようなＭＩログイン画面をクライアントＰＣ１２のディスプレイ５４に表示することで、ＭＩシステム１０にログインするためのユーザＩＤ及びパスワードの入力をユーザに要請する。次のステップ１０２ではユーザからログインの実行が指示されたか判定し、判定が肯定される迄待機する。

【００５７】ＭＩログイン画面には、ユーザＩＤを入力するための入力欄７６、パスワードを入力するための入力欄７８及びログインの実行を指示するためのボタン８０が設けられている。ユーザがクライアントＰＣ１２のキーボード５８やマウス５６を操作することで、入力欄７６にユーザＩＤを、入力欄７８にパスワードを各々入力し、更にボタン８０をクリックすると、ステップ１０２の判定が肯定されてステップ１０４へ移行し、入力されたユーザＩＤ及びパスワードをイントラネット２０を介して運用管理サーバ１６へ送信することで、ＭＩシステム１０へのログインを要求する。ステップ１０６では、ログイン要求に対する応答を運用管理サーバ１６から受信したか否か判定し、判定が肯定される迄待機する。

【００５８】一方、運用管理サーバ１６では、ＣＰＵ１６ＡによってＭＩ運用管理プログラムが実行されることで、図６に示すＭＩ運用管理処理が常時実行されている。このＭＩ運用管理処理では、ステップ１７０でクライアントＰＣ１２等の他のコンピュータから何らかの要

17

求を受信したか否か判定し、判定が肯定される迄待機する。ステップ１７０の判定が肯定されるとステップ１７２へ移行し、他のコンピュータから受信した要求の内容を判定し、判定結果に応じて分岐する。

【００５９】受信した要求が前述のようなクライアントＰＣ１２からのログイン要求であった場合には、ステップ１７２からステップ１７４へ移行する。なお、ステップ１７４～ステップ１９０は本発明の確認・許可手段に対応している。

【００６０】すなわち、ステップ１７４では、クライアントＰＣ１２から受信したユーザＩＤ及びパスワードをキーにしてユーザ情報ＤＢを検索する。また、次のステップ１７６では、ステップ１７４の検索の結果に基づき、受信したユーザＩＤとパスワードの組み合わせがユーザ情報ＤＢに登録されているか否かを判定する。この判定が否定された場合には、今回のログイン要求がＭＩシステム１０の正当なユーザからの要求ではないと判断できるのでステップ１９０へ移行し、ログイン要求元のクライアントＰＣ１２に対し、ユーザＩＤ未登録やパスワード誤り等の理由でログインを受け付けできない旨を通知するエラー応答を送信した後にステップ１７０に戻る。

【００６１】また、ステップ１７６の判定が肯定された場合には、ユーザＩＤ及びパスワードと対応付けられてユーザ情報ＤＢに記憶されている情報（所属部署ＩＤや役職ＩＤ等）をユーザ情報ＤＢから読み出してＲＡＭ１６Ｃ等に一時記憶した後にステップ１７８へ移行し、受信したユーザＩＤをキーにしてログイン管理テーブルを検索する。また、ステップ１８０ではステップ１７８の検索の結果に基づき、受信したユーザＩＤがログイン管理テーブルに登録されているか否か判定する。

【００６２】このログイン管理テーブルは、ＭＩシステム１０に現在ログインしている全ユーザのユーザＩＤを登録するテーブルであり、ステップ１８０の判定が肯定された場合には二重ログインであると判断できるので、ステップ１９０において、ログイン要求元のクライアントＰＣ１２に対して二重ログインを通知するエラー応答を送信した後にステップ１７０に戻る。また、ステップ１８０の判定が否定された場合には、要求されているログインは正当なユーザからの正当なログイン要求であると判断し、ステップ１８２において、先に受信したユーザＩＤをログイン日時等の情報と対応付けてログイン管理テーブルに追加登録する。

【００６３】次のステップ１８４では、ユーザ情報ＤＢから読み出して一時記憶している情報及びユーザＩＤに基づいて、ログインするユーザが利用権限の有るアプリケーション・システムを利用する際に必要となるチケットを生成する。具体的には、例えばユーザＩＤ等のユーザに関する情報に、チケット発行日時や、ユーザが知り得ない所定のマジックワード（例えばバージョン情報）

18

等を付加した後に、一連の情報を秘密鍵によって暗号化することによって生成することができる。

【００６４】また、ステップ１８６ではユーザ情報ＤＢから読み出して一時記憶している権限情報（「利用権限を有するアプリケーション」）に基づき、ログイン要求元のクライアントＰＣ１２のディスプレイ５４に表示するＭＩメニュー画面（一例を図９に示す）を規定するメニュー定義情報を生成する。

【００６５】図９は、ＭＩシステム１０の各アプリケーション・システムのうち、ＲＴＧＳシステム及びＲＡＰＩＤシステムについてのみ利用権限を有しているユーザがログインした際に表示されるＭＩメニュー画面が示されている。図９からも明らかなように、本実施形態に係るＭＩメニュー画面には、ＭＩシステム１０に含まれる各アプリケーション・システムの名称が記されたボタン８２Ａ～８２Ｇが設けられているが、ユーザが利用権限を有しているアプリケーション・システムのボタン８２（図９の例ではボタン８２Ｃ，８２Ｄ）についてのみ、ユーザが利用対象として選択可能なようにアクティブ表示され、ユーザが利用権限を有していないアプリケーション・システムに対応するボタン８２は非アクティブ表示されることで、利用対象として選択できないようになっている。

【００６６】ステップ１８６では、メニュー定義情報に基づいて上記のようなＭＩメニュー画面がクライアントＰＣ１２のディスプレイ５４に表示されるように、メニュー定義情報を生成する。なお、上記のように非アクティブ表示することに代えて、ユーザが利用権限を有していないアプリケーション・システムに対応するボタン８２を表示しないようにしてもよい。

【００６７】そして次のステップ１８８では、生成したチケット及びメニュー定義情報をログイン要求元のクライアントＰＣ１２へ送信することで、ログイン要求に対して正常応答を返し、ステップ１７０に戻る。

【００６８】ＭＩシステム利用処理（図５）では、ステップ１０４でログインを要求してから所定時間以内に運用管理サーバ１６から何らかの応答を受信するか、又は運用管理サーバ１６からの応答がタイムアウトになると、ステップ１０８において、運用管理サーバ１６から正常な応答を受信したか否か判定する。

【００６９】運用管理サーバ１６からエラー応答を受信した場合、或いは運用管理サーバ１６からの応答がタイムアウトになった場合には、判定が否定されてステップ１１２へ移行し、ディスプレイ５４にエラー画面を表示することで、ＭＩシステム１０への通常のログインに失敗したことをユーザに通知する。そして、運用管理サーバ１６からのエラー応答を受信している場合には、受信したエラー応答に基づき、ユーザＩＤ未登録やパスワード誤り等の理由でログインを受け付けできない旨を通知するメッセージを表示したり、或いは二重ログインであ

19

ることを通知するメッセージを表示する。

【００７０】次のステップ１１４では運用管理サーバ１６からの応答がタイムアウトになったか否かに基づいて、運用管理サーバ１６に障害が発生しているか否かを判定する。判定が否定された場合にはステップ１０２に戻り、ユーザＩＤ及びパスワードが入力されてログインの実行が再度指示される迄待機する。なお、ステップ１１４の判定が肯定された場合の処理については後述する。

【００７１】また、運用管理サーバ１６から正常な応答を受信した場合には、ステップ１０８の判定が肯定されてステップ１１０へ移行し、運用管理サーバ１６から受信したチケット及びメニュー定義情報をＨＤＤ６０に記憶する。次のステップ１２２では、ＨＤＤ６０に記憶したメニュー定義画面に基づいて、前述したＭＩメニュー画面（図９参照）をディスプレイ５４に表示する。

【００７２】前述のように、ＭＩメニュー画面は、ユーザが利用権限を有していないアプリケーション・システムは利用対象として選択できないようになっているので、利用権限を有していないアプリケーション・システムをユーザが利用することを阻止することができる。また、複数のアプリケーション・システムの利用権限を有しているユーザが、利用権限を有している複数のアプリケーション・システムを順次又は並列に利用する場合にも、ユーザＩＤ及びパスワードを入力しログインを指示する、というログイン動作を１回行うのみで、単一のクライアントＰＣ１２から複数のアプリケーション・システムを利用することが可能となり、シングル・サインオンを実現できる。

【００７３】ステップ１２４では、ＭＩメニュー画面内の何れかのボタンが選択されたか否か判定し、判定が肯定される迄待機する。オペレータがマウス５６等を操作してＭＩメニュー画面内の何れかのボタンを選択すると、ステップ１２４の判定が肯定されてステップ１２６へ移行し、ユーザによって選択されたボタンが、ボタン８２Ａ～８２Ｇのうちアクティブ表示されている特定のボタン８２か否かに基づいて、利用権限を有する特定のアプリケーション・システムの利用がユーザによって選択されたか否かを判定する。

【００７４】ステップ１２６の判定が肯定された場合にはステップ１２８へ移行し、ＨＤＤ６０に記憶しているチケットを読み出し、読み出したチケットにユーザによる操作の内容を表す情報等を付加し、ユーザによって選択されたボタン８２に対応する特定のアプリケーション・サーバ１４へ送信することで、対応する特定のアプリケーション・システムが提供する各種機能のうち、ユーザの指示に対応する特定機能（例えばＭＩメニュー画面上の対応するボタン８２がユーザによって選択された場合には、特定のアプリケーション・システムのメインメニューをディスプレイ５４に表示させる機能）の利用を

20

要求する。次のステップ１３０では、チケット送信先のアプリケーション・サーバ１４から何らかの応答を受信したか否か判定し、判定が肯定される迄待機する。

【００７５】一方、各アプリケーション・サーバ１４では、ＨＤＤ３０にインストールされているアプリケーション・プログラムがＣＰＵ１４Ａによって実行されることで、図７に示すＭＩアプリケーション処理が各々実行されている。ＭＩアプリケーション処理では、ステップ２１０でクライアントＰＣ１２から特定機能の利用を要求する情報を受信したか否か判定し、判定が肯定される迄待機する。

【００７６】本実施形態において、例えばＲＴＧＳシステムが提供する特定機能をユーザが利用することは、ＭＩメニュー画面上のＲＴＧＳシステムに対応するボタン８２Ｃを選択し、ＲＴＧＳシステムに対応するアプリケーション・サーバ１４により、例として図１０に示すようなＲＴＧＳシステムのメニューバーがディスプレイ５４に表示されている状態で、プルダウンメニューを表示させて所望の項目を選択することによって成される。

【００７７】また、例えばＲＡＰＩＤシステムが提供する特定機能を利用することは、ＭＩメニュー画面上のＲＡＰＩＤシステムに対応するボタン８２Ｄを選択し、ＲＡＰＩＤシステムに対応するアプリケーション・サーバ１４により、例として図１１に示すようなＲＡＰＩＤシステムのメインメニュー画面がディスプレイ５４に表示されている状態で、所望の項目を順次選択することによって成される。

【００７８】ここで、図１０や図１１に示すメニューをディスプレイ５４に表示させることを含め、特定のアプリケーション・システムの特定機能を利用することは、詳しくは、特定機能の利用を要求する操作をユーザが行う毎に、ユーザの操作に応じてクライアントＰＣ１２から対応するアプリケーション・サーバ１４へ特定機能の利用を要求する情報が送信され（前述したステップ１２８）、情報を受信したアプリケーション・サーバ１４が、図７のステップ２１０の判定が肯定されることでステップ２１２以降を実行することによって実現される。

【００７９】図７のフローチャート（のステップ２１２）は、特定機能の利用を要求する情報をクライアントＰＣ１２から受信する毎に個々のアプリケーション・サーバ１４で実行される処理のうちの共通する部分について説明するフローチャートであり、以下では、情報を受信したアプリケーション・サーバ１４（アプリケーション・システム）及び利用が要求された機能を明記することなくステップ２１２以降を説明するが、実際の処理（例えば後述するステップ２２０に相当する処理の内容等）は、情報を受信したアプリケーション・サーバ１４（アプリケーション・システム）及び利用が要求された機能によって大きく相違していることを付記しておく。

【００８０】ステップ２１２では、クライアントＰＣ１

２から受信した情報に含まれるチケットを抽出し、抽出したチケットに基づいて、要求元のクライアントＰＣ１２を操作しているユーザの認証を行う。このユーザ認証は、受信したチケットが運用管理サーバ１６によって発行された正当なチケットか否かを判断することで行うことができ、具体的には、例えば運用管理サーバ１６が暗号化に用いた秘密鍵に対応する公開鍵を用いてチケットを復号化し、復号化によって得られた一連の情報に含まれているユーザＩＤがＨＤＤ３０に記憶されている権限情報ＤＢに登録されているか否かを照合すると共に、前記一連の情報に含まれているマジックワードを正規のマジックワードと照合することで行うことができる。

【００８１】なお、運用管理サーバ１６によって発行されたチケットには有効期限が設けられている。本実施形態では、チケットの有効期限を「運用管理サーバ１６によってチケットが発行されてから２４時間未満」としている。チケットを復号化することで得られる一連の情報にはチケット発行日時が含まれており、ステップ２１２では、チケット発行日時からの経過時間が２４時間未満か否かも判定し、２４時間以上経過していた場合には正当なチケットではないと判断する。この場合、ユーザは、ＭＩシステム１０から一旦ログアウトした後に再度ログインすることで、チケットを再度取得する必要がある。

【００８２】ステップ２１４では、ステップ２１２における認証の結果に基づいて、クライアントＰＣ１２を介して特定機能の利用を要求しているユーザが、対応するアプリケーション・システムの利用権限を有する正当なユーザか否か判定する。受信したチケットが運用管理サーバ１６によって発行された正当なチケットではないと判断された場合には、ステップ２１４の判定が否定されてステップ２３０へ移行し、要求元のクライアントＰＣ１２に対して、ユーザが対応するアプリケーション・システムの利用権限を有していない旨を通知するエラー応答を返し、ステップ２１０に戻る。

【００８３】仮に、所望のアプリケーション・システムが提供する所望の機能を不正に利用しようと目論む者が、クライアントＰＣ１２からアプリケーション・サーバ１４に直接アクセスするための手段を知り得たとしても、上述のように、正当なチケットを所有していなければエラーとなり、そしてチケットを偽造することは極めて困難であるので、アプリケーション・システム側でチケットによるユーザ認証を行うことにより、ＭＩシステム１０にログインすることなくＭＩシステム１０を不正に利用することを阻止することができる。

【００８４】一方、受信したチケットが運用管理サーバ１６によって発行された正当なチケットであると判断された場合にはステップ２１６へ移行し、前記一連の情報に含まれるユーザＩＤを用いて権限情報ＤＢを検索することで、特定機能の利用を要求しているユーザに対応する情報を抽出する。そして、次のステップ２１８において、ステップ２１６の検索によって抽出された情報に基づいて、特定機能の利用を要求しているユーザが特定機能の利用権限を有しているか否か判定する。

【００８５】例えばＲＴＧＳシステムでは、所属部署及び役職毎に利用権限のパターンが定められており、ＲＴＧＳシステムの利用権限を有する個々のユーザの利用権限が何れのパターンに対応しているかを特定するための情報が、個々のユーザのユーザＩＤと対応付けられてＲＴＧＳシステムの権限情報ＤＢに記憶されているので、利用権限の有無の判定は、例えば特定機能の利用を要求しているユーザのユーザＩＤに基づいて、該ユーザの利用権限を表す利用権限パターンを特定し、利用が要求されている特定機能が、前記特定した利用権限パターン上で「利用権限有り」になっているか否かを判断することによって成される。

【００８６】また、例えばＲＡＰＩＤシステムでは、利用権限のパターンがユーザの所属部署及び役職と無関係に作成されるが、ＲＡＰＩＤシステムの利用権限を有する個々のユーザの利用権限が何れのパターンに対応しているかを特定するための情報が、個々のユーザのユーザＩＤと対応付けられてＲＡＰＩＤシステムの権限情報ＤＢに記憶されているので、利用権限の有無の判定は、ＲＴＧＳシステムと同様に、例えば特定機能の利用を要求しているユーザのユーザＩＤに基づいて、該ユーザの利用権限を表す利用権限パターンを特定し、利用が要求されている特定機能が、前記特定した利用権限パターン上で「利用権限有り」になっているか否かを判断することによって成される。

【００８７】更に、例えばＰＹＲＡＭＩＤシステムでは、ユーザに与える利用権限として複数のカテゴリ（表３参照）が存在しているので、利用権限の有無は、例えばユーザから利用を要求されている特定機能が何れのカテゴリに属する機能かを判断し、判断したカテゴリに応じた判定方法で判定される。

【００８８】すなわち、「オペレーション権限」については、「オペレーション権限」に属する各種機能の利用権限がオペレーション権限クラス毎にパターン化されており、ＰＹＲＡＭＩＤシステムの利用権限を有する個々のユーザのオペレーション権限クラスがユーザＩＤと対応付けられてＰＹＲＡＭＩＤシステムの権限情報ＤＢに記憶されているので、ユーザから利用が要求された特定機能が「オペレーション権限」に属する機能であった場合、利用権限の有無の判定は、例えば特定機能の利用を要求しているユーザのユーザＩＤに基づいて、該ユーザのオペレーション権限クラスを特定し、利用が要求されている特定機能が、前記特定したオペレーション権限クラスに対応する利用権限パターン上で「利用権限有り」になっているか否かを判断することによって成される。

【００８９】また「取引オペレーション権限」について

は、「取引オペレーション権限」に属する各種機能の利用権限が取引オペレーション権限クラス毎にパターン化されていると共に、「取引オペレーション権限」に関連する利用権限が所属部署及び管理区分を単位として定められており、ＰＹＲＡＭＩＤシステムの利用権限を有する個々のユーザの取引オペレーション権限クラス、所属部署及び管理区分が、ユーザＩＤと対応付けられてＰＹＲＡＭＩＤシステムの権限情報ＤＢに記憶されている。

【００９０】このため、ユーザから利用が要求された特定機能が「取引オペレーション権限」に属する機能であった場合、利用権限の有無の判定は、例えば特定機能の利用を要求しているユーザのユーザＩＤに基づいて、該ユーザの取引オペレーション権限クラス、所属部署及び管理区分を各々特定し、利用が要求されている特定機能が、前記特定した取引オペレーション権限クラスに対応する利用権限パターン上で「利用権限有り」になっており、かつ特定した所属部署及び管理区分を単位とする利用権限でも利用権限内か否か（すなわち、取引オペレーション権限クラスによって規定される利用権限と所属部署及び管理区分によって規定される利用権限の論理積（ＡＮＤ））を判断することによって成される。

【００９１】特定機能の利用を要求しているユーザが特定機能の利用権限を有していない場合には、ステップ２１８の判定が否定されてステップ２３０へ移行し、要求元のクライアントＰＣ１２に対して、利用が要求された特定機能はユーザの利用権限外である旨を通知するエラー応答を返し、ステップ２１０に戻る。

【００９２】また、利用が要求されている特定機能の利用権限をユーザが有していた場合には、ステップ２１８の判定が肯定されてステップ２２０へ移行し、ユーザの要求に応じて特定機能を提供する処理を行う。この処理としては、例えばユーザがクライアントＰＣ１２のディスプレイ５４への表示を要求した情報をＨＤＤ３０等から読み出す処理、ＨＤＤ３０等に記憶されている情報のうちユーザが更新を指示した情報を更新する処理、ユーザの指示に応じて所定の演算を行う処理、ユーザの指示に応じて他のコンピュータへ所定の情報（電文）を送信する処理等が挙げられる。

【００９３】ステップ２２２では、ステップ２２０で行った処理結果に基づき、該処理の結果を要求元のクライアントＰＣ１２のディスプレイ５４に表示するための画面定義情報を生成する。次のステップ２２４では、ステップ２２２で生成した画面定義情報によって定義される画面内に、ユーザが利用権限を有していない項目（例えばユーザが利用権限を有していない機能を選択するためのボタン等）が有るか否か判定する。

【００９４】ステップ２２４の判定が肯定された場合にはステップ２２６へ移行し、前述のＭＩメニュー画面と同様に、ユーザが利用権限を有していない項目が非アクティブ表示になるように画面定義情報の内容を変更した後にステップ２２８へ移行する。なお、非アクティブ表示にすることに代えて、ディスプレイ５４に表示されないように画面定義情報の内容を変更するようにしてもよい。また、ステップ２２４の判定が否定された場合には、何ら処理を行うことなくステップ２２８へ移行する。そして、ステップ２２８では要求元のクライアントＰＣ１２へ画面定義情報等を送信し、ステップ２１０に戻る。

【００９５】チケット等を送信したクライアントＰＣ１２が送信先のアプリケーション・サーバ１４から何らかの応答を受信すると、ＭＩシステム利用処理（図５）のステップ１３０の判定が肯定され、次のステップ１３２でアプリケーション・サーバ１４からの応答が正常応答か否か判定する。アプリケーション・サーバ１４からの応答がエラー応答の場合には、前記判定が否定されてステップ１３６へ移行し、所定のエラー画面をディスプレイ５４に表示すると共に、受信したエラー応答の内容に応じて、選択されたアプリケーション・システムはユーザの利用権限外である旨を通知するメッセージ、或いは、利用が要求された特定機能はユーザの利用権限外である旨を通知するメッセージを表示する。

【００９６】また、アプリケーション・サーバ１４からの応答が正常応答の場合には、ステップ１３２の判定が肯定されてステップ１３４へ移行し、アプリケーション・サーバ１４から受信した画面定義情報に基づいて、先に特定機能を利用を要求したことに対するアプリケーション・サーバ１４（アプリケーション・システム）の処理結果をディスプレイ５４に表示する。これにより、ユーザが利用を要求した特定機能についての処理結果をユーザが参照又は確認することができる。

【００９７】次のステップ１３８では、アプリケーション・システムが提供する他の特定機能の利用がユーザによって選択されたか否か判定する。判定が否定された場合にはステップ１４０へ移行し、ユーザによってアプリケーション・システムの利用終了が選択されたか否か判定する。この判定も否定された場合にはステップ１３８に戻り、何れかの判定が肯定される迄ステップ１３８，１４０を繰り返す。

【００９８】例えばユーザがキーボード５８やマウス５６等を操作し、ディスプレイ５４に表示された項目のうち、利用したい特定機能に対応する特定項目を選択すると、ステップ１３８の判定が肯定されてステップ１２８に戻り、上述したステップ１２８以降の処理が繰り返されることになる。これにより、ユーザはアプリケーション・システムが提供する各種機能のうち業務の遂行に必要な機能（自身が利用権限を有する機能）を利用しながら、業務を遂行することができる。ユーザによってアプリケーション・システムの利用終了が選択されると、ステップ１４０の判定が肯定されてステップ１２２に戻り、ディスプレイ５４にＭＩメニュー画面が再度表示さ

れる。

【００９９】ところで、ＭＩメニュー画面（図９）には、利用するアプリケーション・システムを選択するためのボタン８２の他に、パスワードを変更するためのボタン８４と、ＭＩシステム１０からログアウトするためのボタン８６も設けられている。また、図９では非アクティブ表示されているが、システム管理者がメインテナンス作業等を行うためのボタン８８も設けられている。

【０１００】ディスプレイ５４にＭＩメニュー画面が表示されている状態で、ユーザによってボタン８２以外のボタンが選択された場合には、ステップ１２２からステップ１２４，１２６を経てステップ１４２へ移行し、ＭＩシステム１０からのログアウトがユーザによって選択されたか否か判定する。

【０１０１】判定が否定された場合にはステップ１５０へ移行し、ユーザが選択したボタンに対応する処理（例えばパスワードを変更するための処理や、システム管理者がメインテナンス等の作業を行うための処理）の実行を運用管理サーバ１６に要求する。これにより、運用管理サーバ１６ではＭＩ運用管理処理（図６）のステップ１７０，１７２を経てステップ１９８へ移行し、クライアントＰＣ１２からの要求に応じた処理を実行する。そして、ユーザが選択したボタンに対応する処理が完了すると、ＭＩシステム利用処理（図５）のステップ１５０からステップ１２２に戻る。

【０１０２】また、ＭＩシステム１０からログアウトするためのボタン８６がユーザによって選択された場合には、ステップ１４２からステップ１４４へ移行し、ＨＤＤ６０に格納していたチケットを廃棄する。ステップ１４６では、運用管理サーバにユーザＩＤを送信してＭＩシステム１０からのログアウトを要求し、次のステップ１４８では応答を受信する迄待機する。

【０１０３】運用管理サーバ１６では、クライアントＰＣ１２からログアウトが要求されると、ＭＩ運用管理処理（図６）のステップ１７０，１７２を経てステップ１９２へ移行する。ステップ１９２では、受信したユーザＩＤをキーにしてログイン管理テーブルを検索し、ステップ１９４ではステップ１９２における検索の結果に基づき、ログイン管理テーブルから該当情報（ユーザＩＤやログイン日時等）を削除する。そして、ログアウト要求元のクライアントＰＣ１２に対し、正常にログアウトできた旨を通知する応答を送信する。

【０１０４】この応答がログアウト要求元のクライアントＰＣ１２で受信されることで、ＭＩシステム利用処理（図５）のステップ１４８の判定が肯定され、ＭＩシステム利用処理の実行が終了する。

【０１０５】続いて、運用管理サーバ１６の応答がタイムアウトになった場合（ＭＩシステム利用処理（図５）のステップ１１４の判定が肯定された場合）の処理について説明する。本実施形態では運用管理サーバ１６が二

重化されているので、運用管理サーバ１６からの応答がタイムアウトになった場合は、運用管理サーバ１６の両系共に障害が発生し応答を返すことができない状態であると判断できる。

【０１０６】このため、ステップ１１４の判定が肯定された場合にはステップ１１６へ移行し、ログインを要求しているユーザによって入力されたユーザＩＤ及びパスワードを障害用サーバ１８へ送信することで、ＭＩシステム１０へのログインを要求する。次のステップ１１８では、障害用サーバ１８から応答を受信したか否か判定し、判定が肯定される迄待機する。

【０１０７】本実施形態では障害用サーバ１８にユーザ情報ＤＢが設けられていないため、クライアントＰＣ１２からログインが要求されると、障害用サーバ１８は障害時用チケット（ユーザＩＤが未設定のチケット）を生成し、ログイン要求元のクライアントＰＣ１２へ送信する。障害用サーバ１８に対してログインを要求したクライアントＰＣ１２は、障害用サーバ１８から障害時用チケットを受信すると、ステップ１１８の判定が肯定されてステップ１２０へ移行し、受信した障害時用チケットにログインを要求しているユーザのユーザＩＤを設定し、ＨＤＤ６０に格納した後にステップ１２２へ移行する。

【０１０８】これにより、運用管理サーバ１６に障害が発生し正規のチケットが発行されない場合にも、障害用サーバ１８によって発行される障害時用チケットを用いることで、ＭＩシステム１０の各アプリケーション・システムを利用することができる。また、運用管理サーバ１６に障害が発生している際にも、各アプリケーション・システムにおいて、ユーザＩＤに基づく利用権限のチェックが行われるので、ユーザが利用権限外のアプリケーション・システムを利用したり、利用権限外の機能を利用することを阻止することができる。

【０１０９】なお、上記ではＭＩシステム１０を利用するための専用プログラム（ＭＩシステム利用プログラム）がクライアントＰＣ１２にインストールされており、このプログラムに従ってクライアントＰＣ１２がＭＩシステム利用処理を行うことで、ＭＩシステム１０の利用が可能となる場合を例に説明したが、本発明はこれに限定されるものではなく、例えばクライアントＰＣ１２にブラウザ等の一般的なプログラムのみがインストールされている環境下でも本発明は実現可能である。

【０１１０】また、上記ではＭＩシステム１０に含まれる全てのアプリケーション・システムに各ユーザ毎の利用権限を規定する権限情報ＤＢが設けられており、各アプリケーション・システムは、ユーザから特定機能の利用が要求される毎に、チケットを用いたユーザ認証を行うと共に、権限情報ＤＢに基づきユーザが特定機能の利用権限を有しているか否かを判定する場合を説明したが、これに限定されるものではなく、本発明に係るコン

27

ピュータ・システムの中に、個々のユーザの利用権限が一定のアプリケーション・システム（例えば提供可能な全機能を全ユーザに提供するアプリケーション・システム）が含まれていてもよい。この場合、利用権限の判定は省略可能であるが、セキュリティ性確保のためにチケットを用いたユーザ認証は省略しないことが望ましい。

【０１１１】また、上記では金融機関のコンピュータ・システムに本発明を適用した例を説明したが、これに限定されるものではなく、本発明は、複数のアプリケーション・システムを含んで構成された任意のコンピュータ・システムに適用可能であることは言うまでもない。

【０１１２】

【発明の効果】以上説明したように請求項１及び請求項９記載の発明は、コンピュータ・システムを利用可能な個々のユーザを確認するためのユーザ情報と、個々のユーザが利用権限を有しているアプリケーション・システムを特定するための第１権限情報を第１記憶手段に記憶すると共に、アプリケーション・システムに対応して設けられた第２記憶手段に、対応するアプリケーション・システムが提供可能な複数種の機能のうち、個々のユーザが利用権限を有している機能を特定するための第２権限情報を記憶し、コンピュータ・システムへのユーザのログイン要求に対し、ユーザ情報に基づいてユーザの確認を行い、正当な利用者であることを確認できたユーザに対し、第１権限情報に基づき前記ユーザが利用権限を有しているアプリケーション・システムについてのみ利用を許可し、アプリケーション・システムは、自システムがユーザに提供可能な機能の利用を要求しているユーザに対し、第２権限情報に基づき、前記ユーザが利用権限を有している機能のみを前記ユーザに提供するので、個々のユーザ毎に定められた利用権限に従って個々のユーザによるシステムの利用をコントロールすることを、メインテナンス性やセキュリティ性を損なうことなく実現できる、という優れた効果を有する。

【０１１３】請求項５記載の発明は、請求項１記載の発明において、アプリケーション・システムは、提供可能な複数種の機能のうちの何れかの機能の利用がユーザから要求される毎に、要求されている機能の利用権限をユーザが有しているか否かを判断するので、上記効果に加え、各アプリケーション・システムが提供可能な個々の機能が、利用権限のないユーザによって不正に利用されることを確実に阻止することができる、という効果を有する。

【０１１４】請求項６記載の発明は、請求項１記載の発明において、正当な利用者であることを確認できたユーザに対してチケット情報を与え、各アプリケーション・システムは、提供可能な機能の利用を要求しているユーザが正当なチケット情報を所持しているか否かを判断することで、前記ユーザが正当な利用者か否かを判定するので、上記効果に加え、確認・許可手段による正当な利用者であることの確認を経ることなく、コンピュータ・システムが不正利用されることを阻止することができる、という効果を有する。

28

【０１１５】請求項８記載の発明は、請求項６記載の発明において、確認・許可手段に異常が生じた場合に、コンピュータ・システムへのユーザのログイン要求に対し、障害用チケット情報をユーザに与えるようにしたので、上記効果に加え、確認・許可手段に異常が生じた場合にも、正当な利用者が全てのアプリケーション・システムを利用できない状態に陥ることを回避できる、という効果を有する。

【図面の簡単な説明】

【図１】　本実施形態に係るコンピュータ・システムの概略構成を示すブロック図である。

【図２】　ＲＴＧＳシステムのユーザ情報設定画面の一例を示すイメージ図である。

【図３】　ＲＡＰＩＤシステムのユーザ情報設定画面の一例を示すイメージ図である。

【図４】　ＲＡＰＩＤシステムのユーザ情報設定画面の一例を示すイメージ図である。

【図５】　クライアントＰＣで実行されるＭＩシステム利用処理の内容を示すフローチャートである。

【図６】　運用管理サーバで実行されるＭＩ運用管理処理の内容を示すフローチャートである。

【図７】　アプリケーション・サーバで実行されるＭＩアプリケーション処理の内容を示すフローチャートである。

【図８】　ＭＩログイン画面の一例を示すイメージ図である。

【図９】　ＭＩメニュー画面の一例を示すイメージ図である。

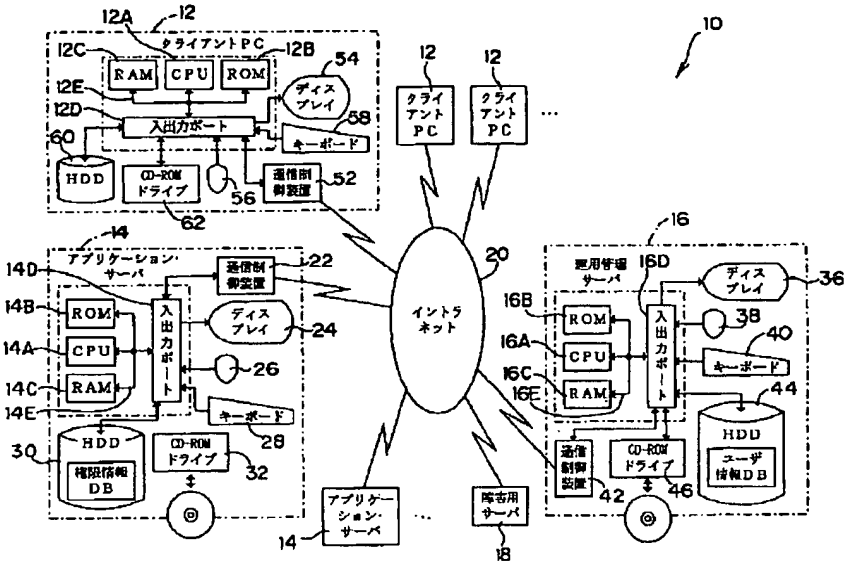
【図１０】　ＲＴＧＳシステムのメニューバーの一例を示すイメージ図である。

【図１１】　ＲＡＰＩＤシステムのメインメニュー画面の一例を示すイメージ図である。

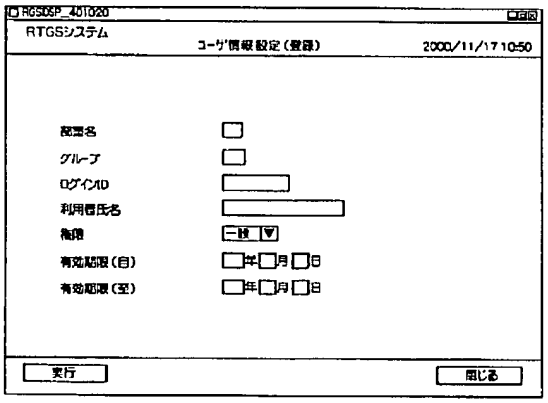
【符号の説明】

１０　コンピュータ・システム
１２　クライアントＰＣ
１４　アプリケーション・サーバ
１６　運用管理サーバ
１８　障害用サーバ
２０　イントラネット
３０　ＨＤＤ
４４　ＨＤＤ
５４　ディスプレイ
５６　マウス
５８　キーボード

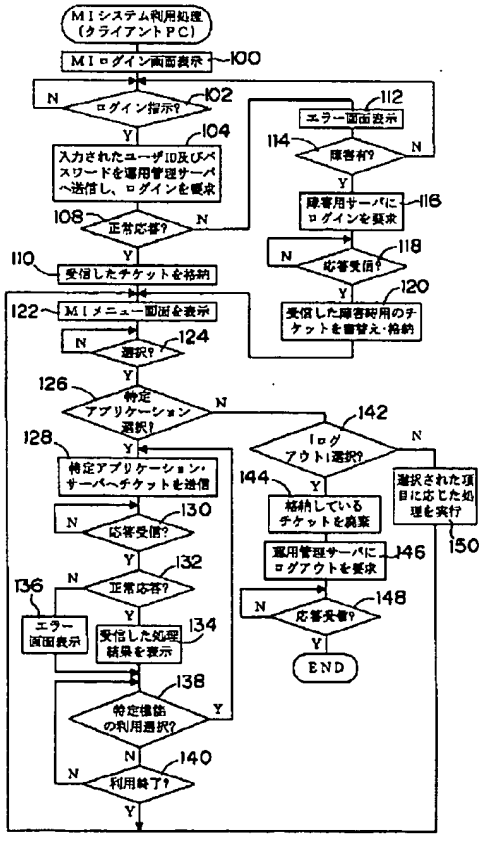
【図１】


12A
12
クライアントPC
12C
12B
RAM
CPU
ROM
54
ディスプレイ
12E
12D
入出力ポート
58
キーボード
60
HDD
CD-ROMドライブ
56
通信制御装置
52
62
10
12
12
クライアントPC
クライアントPC
...
14
アプリケーションサーバ
140
通信制御装置
22
14B
ROM
14A
CPU
14C
RAM
14E
入出力ポート
ディスプレイ
24
26
キーボード
28
HDD
権限情報DB
30
CD-ROMドライブ
32
20
イントラネット
16
運用管理サーバ
16D
ディスプレイ
36
16B
ROM
16A
CPU
16C
RAM
16E
入出力ポート
38
40
キーボード
44
HDD
ユーザ情報DB
通信制御装置
42
CD-ROMドライブ
46
アプリケーションサーバ
14
...
障害用サーバ
18

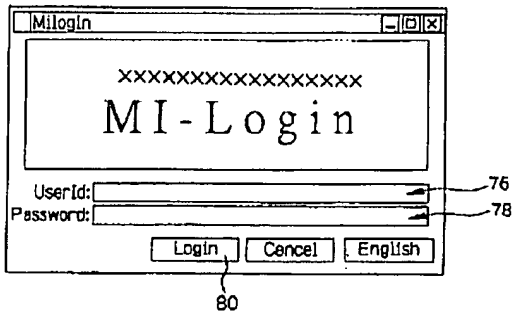
【図２】


RGSDSP_401020
RTGSシステム
ユーザ情報設定(登録)
2000/11/17 10:50
配置名
グループ
ログインID
利用者氏名
権限
有効期限(自)
有効期限(至)
実行
閉じる

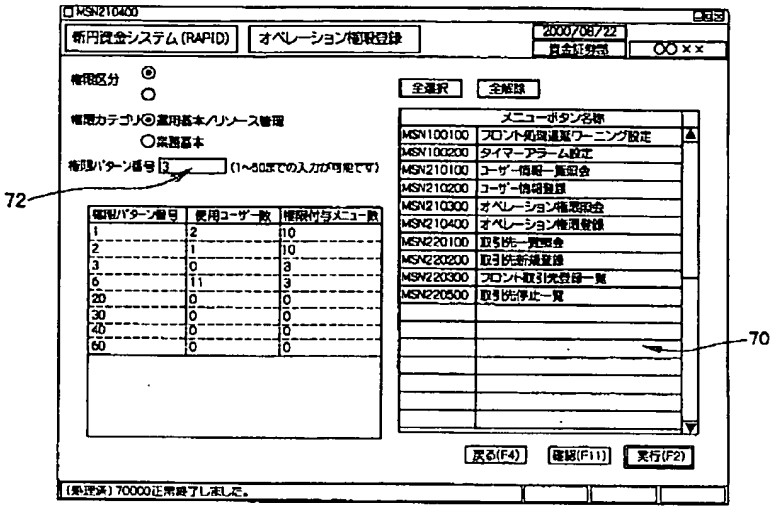
【図５】


MIシステム利用処理(クライアントPC)
MIログイン画面表示
100
ログイン指示?
102
入力されたユーザID及びパスワードを運用管理サーバへ送信し、ログインを要求
104
正常応答?
108
受信したチケットを格納
110
MIメニュー画面を表示
122
選択?
124
特定アプリケーション選択?
126
特定アプリケーション・サーバへチケットを送信
128
応答受信?
130
正常応答?
132
エラー画面表示
136
受信した処理結果を表示
134
特定機器の利用選択?
138
利用終了?
140
エラー画面表示
112
障害有?
114
障害用サーバにログインを要求
116
応答受信?
118
受信した障害対応用のチケットを書替え・格納
120
ログアウト選択?
142
格納しているチケットを廃棄
144
運用管理サーバにログアウトを要求
146
応答受信?
148
END
選択された項目に応じた処理を実行
150

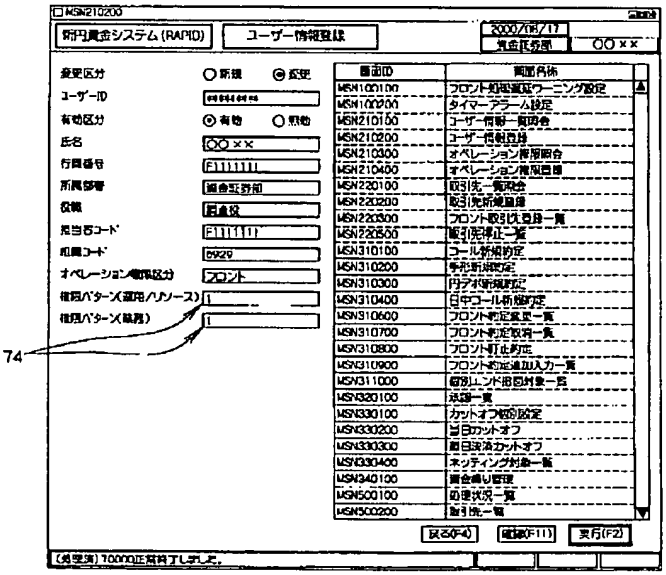
【図８】


MiLogIn
XXXXXXXXXXXXXXXXX
MI-Login
UserId:
76
Password:
78
Login
Cancel
English
80

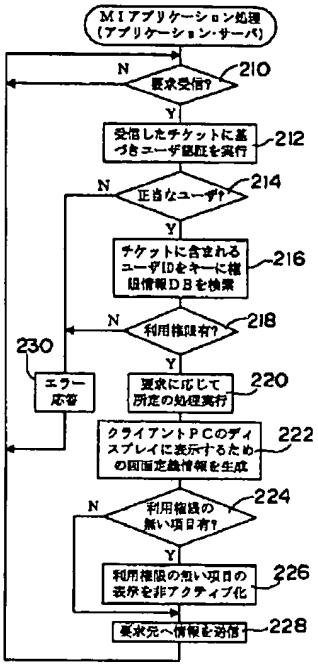
【図３】


MSN210400
新円資金システム(RAPID)
オペレーション権限登録
2000/08/22
権限区分
全選択
全解除
権限カテゴリ◉運用基本/リソース管理
○業務基本
権限パターン番号
(1～60までの入力が可能です)
72
権限パターン番号
使用ユーザー数
権限付与メニュー数
メニューボタン名称
MSN100100 フロント処理遅延ワーニング設定
MSN100200 タイマーアラーム設定
MSN210100 ユーザー情報一覧照会
MSN210200 ユーザー情報登録
MSN210300 オペレーション権限照会
MSN210400 オペレーション権限登録
MSN220100 取引先一覧照会
MSN220200 取引先新規登録
MSN220300 フロント取引先登録一覧
MSN220500 取引先停止一覧
70
戻る(F4)
確認(F11)
実行(F2)
(処理済) 70000正常終了しました。

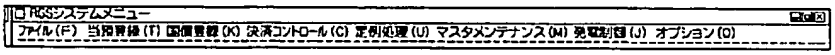
【図４】


MSN210200
新円資金システム(RAPID)
ユーザー情報登録
2000/08/17
変更区分
○新規 ◉変更
ユーザーID
有効区分
◉有効 ○無効
氏名
行員番号
所属部署
役職
担当者コード
組織コード
オペレーション権限区分
フロント
権限パターン(運用/リソース)
権限パターン(業務)
74
画面ID
画面名称
MSN100100 フロント処理遅延ワーニング設定
MSN100200 タイマーアラーム設定
MSN210100 ユーザー情報一覧照会
MSN210200 ユーザー情報登録
MSN210300 オペレーション権限照会
MSN210400 オペレーション権限登録
MSN220100 取引先一覧照会
MSN220200 取引先新規登録
MSN220300 フロント取引先登録一覧
MSN220500 取引先停止一覧
MSN310100 コール新規約定
MSN310200 予約新規設定
MSN310300 円デポ新規約定
MSN310400 日中コール新規約定
MSN310600 フロント約定照会一覧
MSN310700 フロント約定取消一覧
MSN310800 フロント訂正約定
MSN310900 フロント約定追加入力一覧
MSN311000 個別ユーロ相場対象一覧
MSN320100 通貨一覧
MSN330100 カットオフ時刻設定
MSN330200 当日カットオフ
MSN330300 翌日決済カットオフ
MSN330400 ネッティング対象一覧
MSN340100 資金繰り管理
MSN500100 処理状況一覧
MSN500200 取引先一覧
戻る(F4)
確認(F11)
実行(F2)
(処理済) 70000正常終了しました。

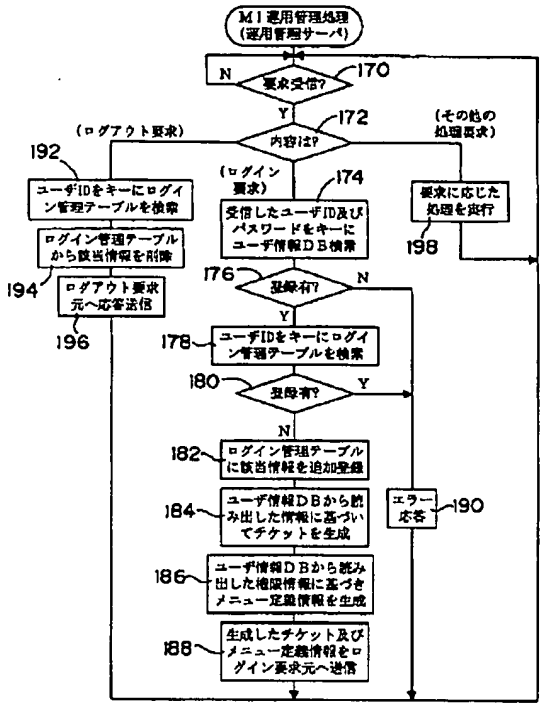
【図７】


ＭＩアプリケーション処理
(アプリケーション・サーバ)
要求受信?
210
N
Y
受信したチケットに基づきユーザ認証を実行
212
正当なユーザ?
214
チケットに含まれるユーザIDをキーに権限情報ＤＢを検索
216
利用権限有?
218
230
エラー応答
要求に応じて所定の処理実行
220
クライアントＰＣのディスプレイに表示するための画面定義情報を生成
222
利用権限の無い項目有?
224
利用権限の無い項目の表示を非アクティブ化
226
要求元へ情報を送信
228

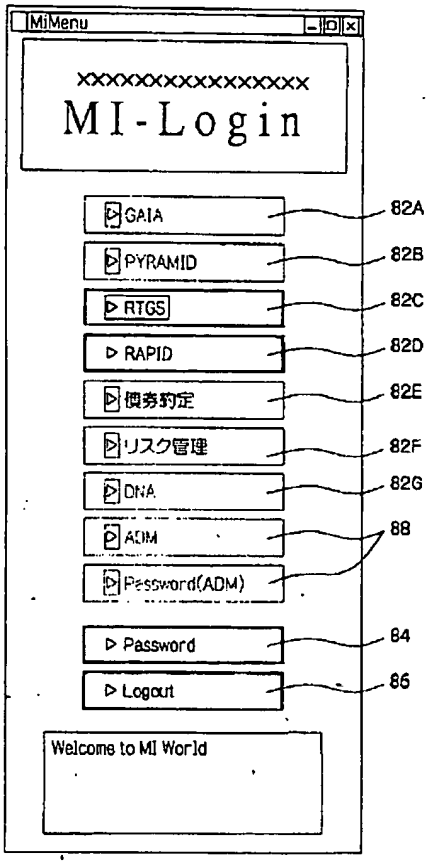
【図１０】


RGSシステムメニュー
ファイル(F) 当預貸金(T) 国債管理(K) 決済コントロール(C) 定例処理(U) マスタメンテナンス(M) 免責制限(J) オプション(O)

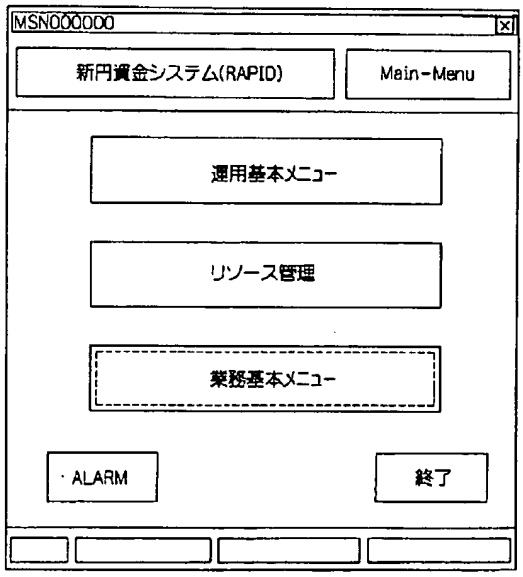
【図６】


MI運用管理処理
(運用管理サーバ)
N
要求受信?
170
Y
内容は?
172
(ログアウト要求)
(ログイン要求)
(その他の処理要求)
192
ユーザIDをキーにログイン管理テーブルを検索
174
受信したユーザID及びパスワードをキーにユーザ情報DB検索
要求に応じた処理を実行
198
ログイン管理テーブルから該当情報を削除
194
ログアウト要求元へ応答送信
196
176
登録有?
N
Y
178
ユーザIDをキーにログイン管理テーブルを検索
180
登録有?
Y
N
182
ログイン管理テーブルに該当情報を追加登録
184
ユーザ情報DBから読み出した情報に基づいてチケットを生成
エラー応答
190
186
ユーザ情報DBから読み出した権限情報に基づきメニュー定義情報を生成
188
生成したチケット及びメニュー定義情報をログイン要求元へ送信

【図９】


MiMenu
xxxxxxxxxxxxxxxx
MI-Login
GAIA
82A
PYRAMID
82B
RTGS
82C
RAPID
82D
債券判定
82E
リスク管理
82F
DNA
82G
ADM
88
Password(ADM)
Password
84
Logout
86
Welcome to MI World

【図１１】


MSN000000
新円資金システム(RAPID)
Main-Menu
運用基本メニュー
リソース管理
業務基本メニュー
ALARM
終了